Dual WAN Firewall Router

VPN 800 / 2

User's Guide

HotBrick Network Solutions

TABLE OF CONTENTS

Document Version: 1.4

1: Introduction

Congratulations on the purchase of your new HotBrick VPN 800/2 Firewall Router. The VPN 800/2 Firewall Router provides ***Shared Broadband Internet Access*** and ***VPN tunnels*** for LAN users.

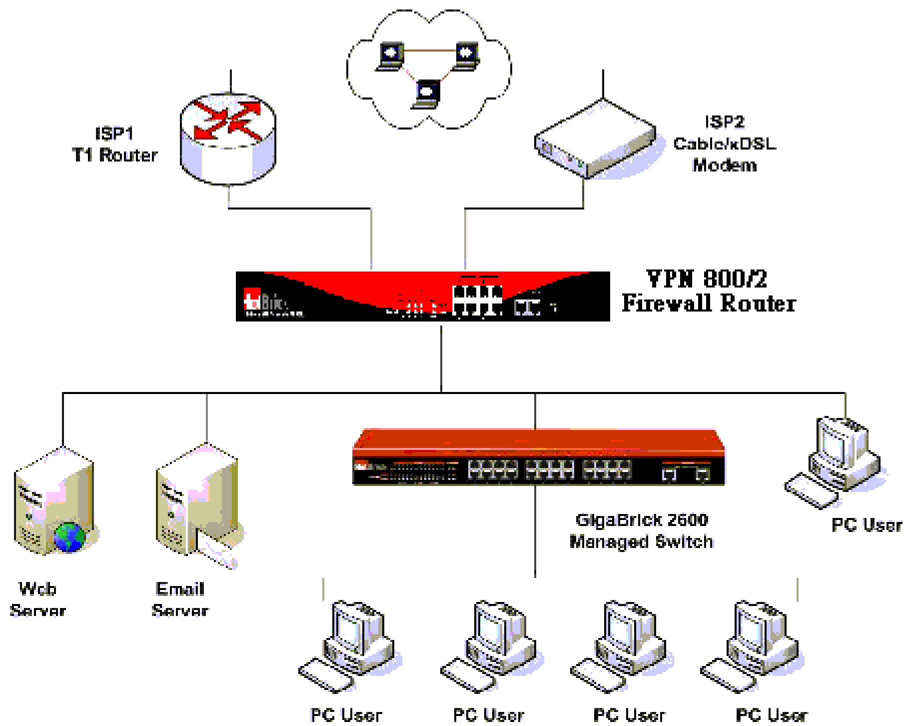


Figure 1-1: VPN 800/2 Firewall Router

Internet Features

- ***Shared Broadband Internet Access***

  All LAN users can access the Internet through the VPN 800/2 Firewall Router, by sharing one (1) or two (2) Broadband modems and connections.

- ***High-Performance Dual Modem Support***

  The VPN 800/2 Firewall Router has two (2) WAN ports, allowing connection of two (2) Broadband modems.
  This gives twice the bandwidth of a single modem.
  Flexible configuration allows each port to use a different type of modem and connection method. Also, you can determine how the Internet traffic is shared between the 2 modems.

- ***Supports all common Connection Methods***

  All popular DSL and Cable Modems and connection methods are supported, including Fixed IP, Dynamic IP, PPPoE, and PPTP.

- ***PPPoE Session Management***

  Multiple PPPoE sessions are supported and you can choose to “map” sessions to individual PCs if desired.

- ***Multiple IP Address Support***

  If your ISP allocates you multiple IP addresses, these are also supported and you can “map” IP addresses to individual PCs if desired.

- ***Special Applications***

  This feature allows you to use some non-standard applications, where the port number used for the response is different to the port number used by the sender.

- ***Virtual Servers***

  This feature allows Internet users to access Internet servers on your LAN. For standard servers such as Web, FTP or E-Mail servers, only the IP address of the server PC is required. You can also define you own Server types if required.

- ***Multiple DMZ***

  A "DMZ" PC will receive incoming connection requests, which would otherwise be blocked. For each IP address allocated by your ISP, a separate "DMZ" PC can be specified. So if your ISP has given you multiple IP addresses, you can have multiple “DMZ” PCs. Each “DMZ” PC has unrestricted 2-way Internet access, providing the ability to run programs that are otherwise incompatible with NAT routers like the Load Balancer.

- ***Access Filter***

  The network Administrator can use the Access Filter to gain fine control over the Internet access and applications available to LAN users. Five (5) user groups are available, and each group can have different access rights.

- ***Block URL***

  Use this feature to block access to undesirable Web sites by LAN users. You can even have different settings for different groups of PCs.

- ***Session Limit***

  With Session Limit feature, if the numbers of new sessions for system exceed the maximum in the sampling time, any new session in the system will be drop.

- ***System Filter Exception***

  With firewall exception, the packets will not be processed by firewall or NAT module, but be processed directly by system protocol stack.

Other Features

- ***8-Port Switching Hub***

  The VPN 800/2 Firewall Router incorporates with 8-port 10 /100BaseT switching hub, making it easy to create or extend your LAN.

- ***DHCP Server Support***

  Dynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The VPN 800/2 Firewall Router acts as a **DHCP Server** for devices on your local LAN.

- ***Multi Segment LAN Support***

  LANs containing one or more segments are supported, via the VPN 800/2 Firewall Router's built-in static routing table.

- ***ARP proxy***

  The ARP proxy feature allows you to assign an external (Internet) IP address to the VPN 800/2 Firewall Router's LAN port. This allows Servers on your LAN to have external (Internet) IP addresses.

- ***Easy Setup***

  Use your favorite WEB browser for configuration.

- ***Remote Management***

  The VPN 800/2 Firewall Router can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

- ***Password - protected Configuration***

  Optional password protection is provided to prevent unauthorized users from modifying the configuration data and settings.

- ***HTTP Firmware Upgrade and backup***

  The web management feature allows you to use HTTP upgrade new firmware and backup system configuration from local or even from remote site. As long as you enable “Remote upgrade” and “Remote web-based setup” from Advanced feature web page.

- ***Email Alert***

  It will send a warning email to the system administrator, if one of the WAN ports was disconnected when both WAN ports are enabled.

- ***Syslog***

  It can generate real time system information on the web page or a particular machine. It is useful to monitor the device.

- ***QoS Configuration.***

  This function will make some specified packets with higher priority for pass-through. Especially you use real-time applications like Internet phone, videoconference, etc.

- ***UPnP***

  To “Enable” UpnP (Universal Plug & Play), the load balancer will become one of the network devices. It is useful to discovery and control network devices, such as Internet gateway.

Package Contents

The following items should be included:

- The VPN 800/2 Firewall Router Unit
- Power Cord.
- Quick Installation Guide
- CD-ROM containing the on-line manual.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Front Panel

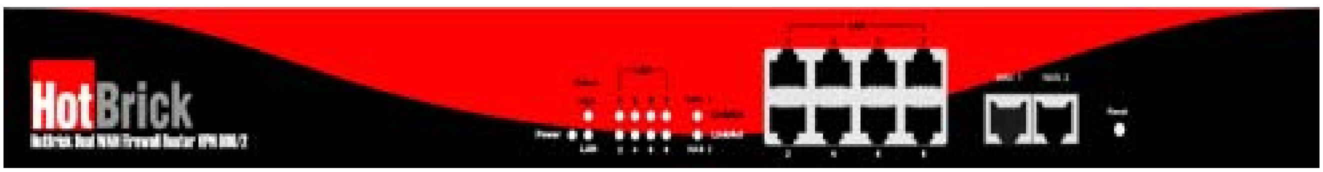


Figure 1-2: Front Panel VPN 800/2 Firewall Router

Operation of the Front Panel LEDs is as follows:

LAN LED	
100M (Green)	ON – The corresponding LAN port is using 100BaseT.
	OFF – No physical connection.
10M (Yellow)	ON – The corresponding LAN port is using 10BaseT.
	OFF – No physical connection.
WAN LED	Green : 100M
	Yellow: 10M
	Flash: Active
Status LED	
WAN Status	Green Flash: WAN Active
LAN Status	Yellow: Error
	Green Flash: LAN Active
	Yellow: Error
	Blinking – Data in/out
Reset Button	When pressed the reset button around 3 seconds, and release it. The VPN 800/2 Firewall Router will reset to factory default value.

Also, some Status and Error conditions are indicated by combinations of LEDs, as shown below

LED Action	Condition
WAN, LAN Status LEDs flash alternatively.	Firmware Download in progress.
WAN & LAN LEDs flash concurrently.	MAC address not assigned.

Caution:

To re-plug the VPN 800/2 Firewall Router,it should be apart from unplug time more than 20 seconds.

Rear Panel VPN 800/2 Firewall Router



Figure 1-3: Rear Panel VPN 800/2 Firewall Router

AC power socket	Connect the supplied power here.

Default Settings

When the VPN 800/2 Firewall Router has finished booting, all configuration settings will be set to the factory defaults, including:

- *IP Address* set to its default value of 192.168.1.1, with a *Network Mask* of 255.255.255.0
- *DHCP Server* is enabled
- *User Name: admin*
- Password cleared (no password)

TFTP Download

This setting should be used only if your VPN 800/2 Firewall Router is unusable, and you wish to restore it by downloading new firmware. Follow this procedure:

1. Power On the VPN 800/2 Firewall Router.
2. Use the supplied Windows utility or a TFTP client program applies the new firmware. If using the supplied Windows TFTP program, the screen will look like the following example.

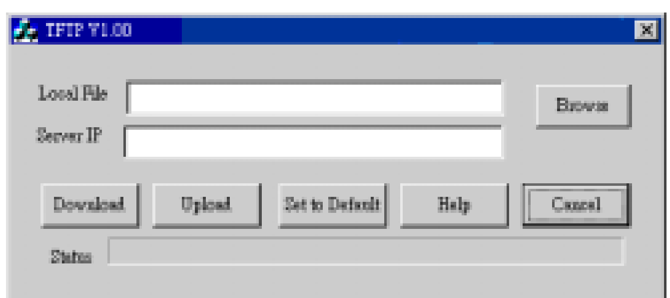


Figure 1-4: Windows TFTP utility VPN F 800/2 Firewall Router

- Enter the name of the firmware upgrade file on your PC, or click the "Browse" button to locate the file.
- Enter the LAN IP address of the VPN 800/2 Firewall Router in the "Server IP" field.
- Click "Download" to send the file to the VPN 800/2 Firewall Router.

3. When downloading is finished. It should then work normally, using the default settings.

Note:

The supplied Windows TFTP utility also allows you to perform three (3) other operations:

- Save the current configuration settings to your PC (use the "Upload" button).
- Restore a previously saved configuration file to the VPN 800/2 Firewall Router (use the "Download" button).
- VPN 800/2 Firewall Router to its default values (use the "Set to Default" button).

2: Basic Setup

Overview

Basic Setup of your HotBrick VPN 800/2 Firewall Router involves the following steps:

1. Attach the HotBrick VPN 800/2 Firewall Router to one (1) PC, and configure it for your LAN.
2. Install your HotBrick VPN 800/2 Firewall Router in your LAN, and connect the Broadband Modem or Modems.
3. Configure your HotBrick VPN 800/2 Firewall Router Internet Access.
4. Configure PCs on your LAN to use the VPN 800/2 Firewall Router.

Requirements

- One (1) or two (2) DSL or Cable modems, each with an Internet Access account with an ISP.
- Network cables. Use standard 10/100BaseT network (UTP) cables with RJ45 connectors
- TCP/IP network protocol must be installed on all PCs.

Procedure

1: Configuring the VPN 800/2 Firewall Router for your LAN

1. Use a standard LAN cable to connect your PC to any Hub port on the VPN 800/2 Firewall Router.
2. Connect the power cord and power up the VPN 800/2 Firewall Router. Only use the power cord provided; using a different one may cause hardware damage.
3. Start your PC. If your PC is already running, restart it. It will then obtain an IP address from the VPN 800/2 Firewall Router.
4. Start your WEB browser.
5. In the *Address* or *Location* box enter:

   `HTTP://192.168.1.1`

6. You will be prompted for the User Name and password, as shown below.

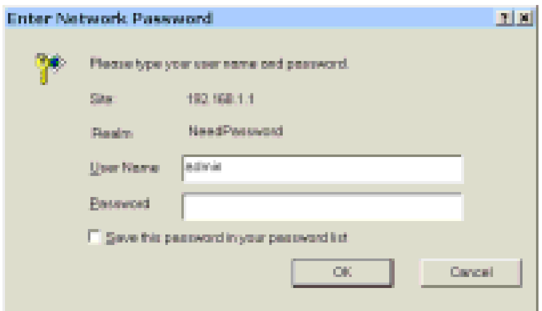


Figure 2-1: Password Dialog

7. Enter *admin* for the "User Name" and leave the "Password" blank.
    - The "User Name" is always *admin*
    - You can and should set a password, using the following ***Admin Password*** screen.

No Response?

- Is your PC using a Fixed IP address?

  If so, you must configure your PC to use an IP address within the range 192.168.1.2 to 192.168.1.254, with a *Network Mask* of 255.255.255.0. See *Appendix B – Windows TCP/IP Setup* for details.
- Check that the VPN 800/2 Firewall Router is properly installed, LAN connection is OK, and it is powered ON.

8. After the login, you will then see the ***Admin Password*** screen, as shown below.
   Assign a password by entering it in the "Password" and "Verify Fields.

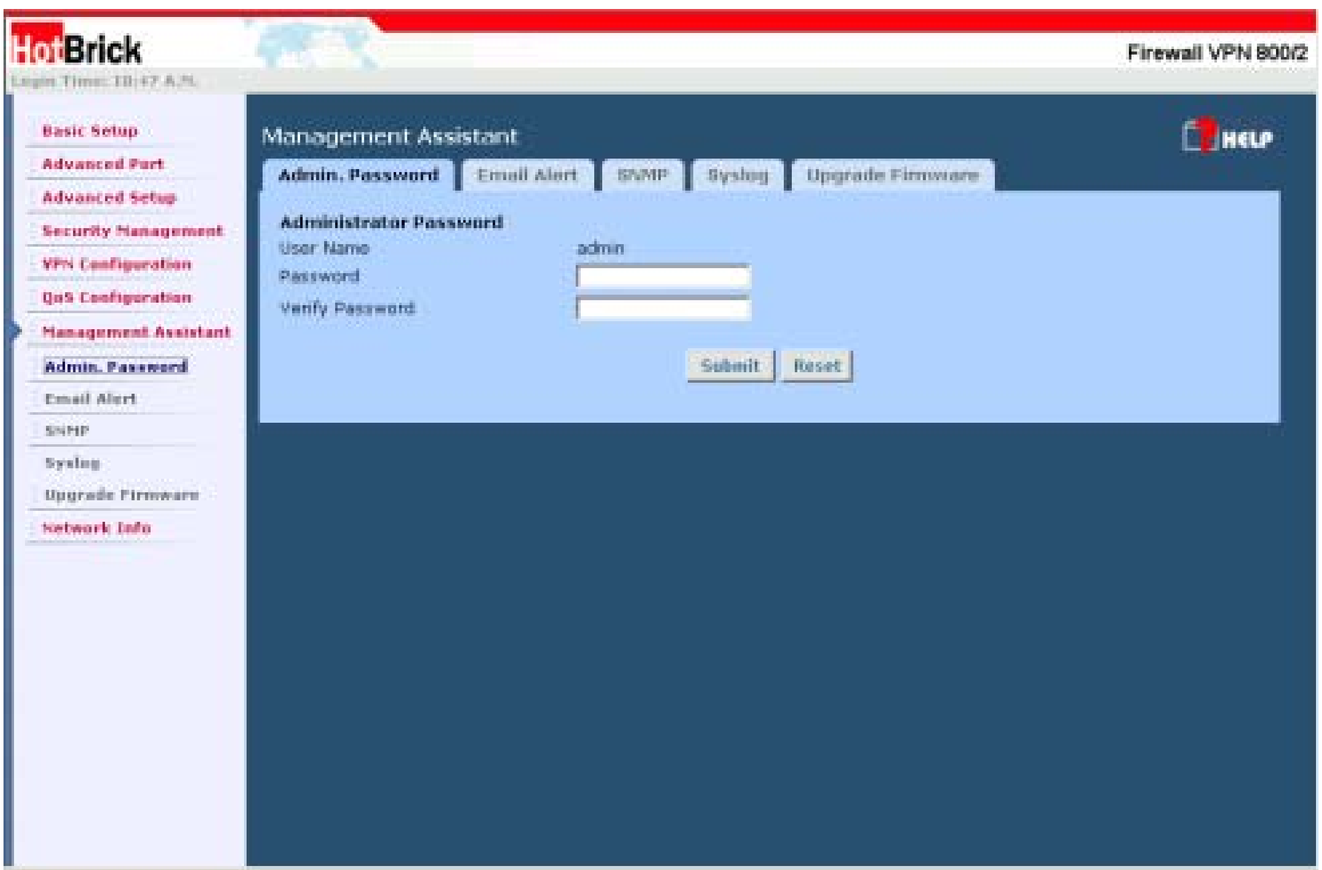


Figure 2-2: Home Screen (Admin Password) VPN 800 /2

9. Select ***LAN & DHCP*** from the menu. You will see a screen like the example below.

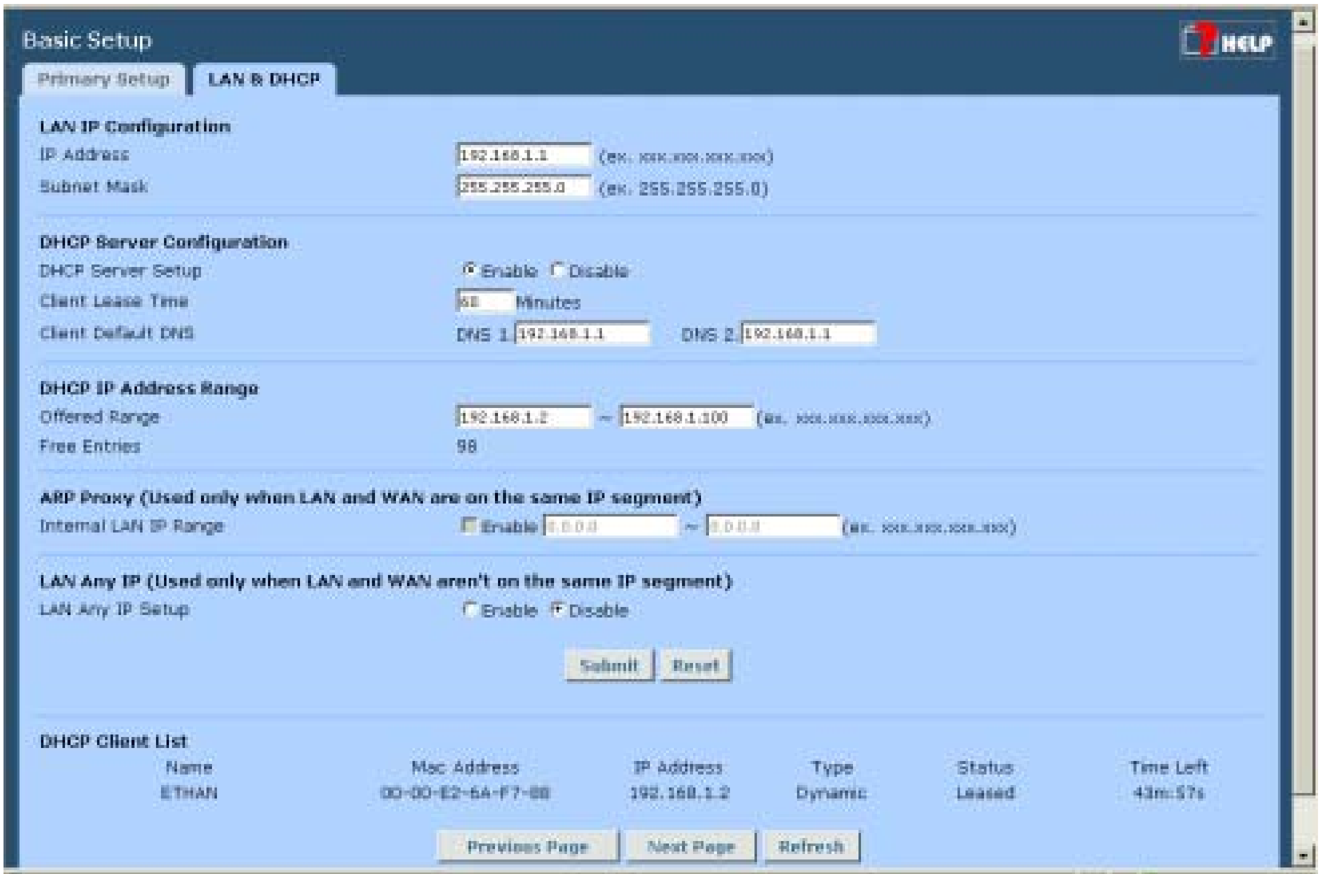


Figure 2-3: LAN & DHCP

10. Ensure these settings are suitable for your LAN:
    - The default settings are suitable for many situations.
    - See the following table for details of each setting.
11. Save your data, then go to *Step 2, Installing the* VPN 800/2 Firewall Router *in your LAN*.

Settings – LAN & DHCP

LAN IP Configuration	**IP address** - for the VPN 800/2 Firewall Router, as seen from the local LAN. Use the default value unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN. **Subnet Mask** -The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Subnet Mask for the LAN segment to which the VPN 800/2 Firewall Router is attached (the same value as the PCs on that LAN segment).

DHCP Server Configuration	• **DHCP Server Setup** - If **enabled**, the VPN 800/2 Firewall Router will allocate IP Addresses to PCs (DHCP clients) on your LAN when they start up. The default and recommended value is "Enable". (Windows systems, by default, act as DHCP clients. This setting is called *Obtain an IP address automatically*.) • **DHCP Server Setup** - If you are already using a DHCP Server, the DHCP Server setting must be **disabled**, and the existing DHCP server must be set to provide the IP address of the VPN 800/2 Firewall Router as the *Default Gateway*. • **Client Lease Time** – It is a finite period of time for a DHCP server lease an IP address to a client. • **Client Default DNS** – An IP address of the default DNS server for the client requesting DHCP service.
DHCP IP Address Range	• **Offered Range** fields set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. • **Free Entries** indicates how many DHCP entries are not currently allocated, and still available.
ARP Proxy	Enable this ONLY if the LAN port has an IP address in the same address range as the WAN port(s). This means that all PCs using this Gateway must have valid fixed external (Internet) IP addresses. If enabled, enter the IP address range used on your LAN.
LAN Any IP Setup	By default is disabled. If you enable “LAN any IP”, that means no matter what static IP address hold on the client (your PC). The clients do not need to change the IP address, even though it has different IP segment than LAN segment, it still can access Internet through NAT.
DHCP Client List	This table shows the IP addresses which have been allocated by the DHCP Server function. For each address, which has been allocated, the following information is shown. • **Name** – The "hostname" of the PC. In some cases, this may not be known. • **MAC Address** – The physical address (network adapter address) of the PC. • **IP Address** – The IP address allocated to this PC. • **Type** – Indicates IP address to be dynamic or static. • **Status** – If *Dynamic*, the IP address was allocated by this DHCP Server. If *Sniffed*, the IP address was detected by examining the LAN, rather than allocated by the DHCP Server. In this case, the *Name* is usually not known. • **Time Left** – The time expired since which IP address is leased.

2. Installing the HotBrick VPN 800/2 Firewall Router in your LAN

1. Ensure the HotBrick VPN 800/2 Firewall Router and the DSL/Cable modem are powered OFF. Leave the modem or modems connected to their data line.
2. Connect the Broadband modem or modems to the VPN 800/2 Firewall Router.
   - If using only one (1) Broadband modem, connect it to the "WAN 1" port.
   - Use the cable supplied with your DSL/Cable modem. If no cable was supplied, use a standard cable.
3. Use standard LAN cables to connect PCs to the Switching Hub ports on the VPN 800/2 Firewall Router.
   - Both 10BaseT and 100BaseT connections can be used simultaneously.
   - If you need to connect the VPN 800/2 Firewall Router to another Hub, just use a standard LAN cable to connect any port on the VPN 800/2 Firewall Router to a standard port on another hub. Any LAN port on the VPN 800/2 Firewall Router will automatically act as an "Uplink" port when required.
4. Power Up
   - Power on the Cable or DSL modem or modems.
   - Connect the supplied power cord to the VPN 800/2 Firewall Router and power up.
5. Check the LEDs
   - The ***Power*** LED should be ON.
   - The ***WAN – Link*** LED should be ON, if the corresponding WAN port is connected to a broadband modem.
   - The ***Error*** LED will flash during start up, but will then turn off. If it stays on, there is an error condition.
   - For each PC connected to the LAN ports, the corresponding ***LAN*** LED (either ***10*** or ***100***) should be ON.

3. Configuring the HotBrick VPN 800/2 Firewall Router for Internet Access

Select *Primary Setup* from the menu, to see a screen like the example below.

- Configure WAN 1 and/or WAN 2 as required.
- For any of the following situations, refer to ***Chapter 3: Advanced Port Setup*** for any further configuration, which may be required.
  - Using both ports
  - Multiple IP addresses on either port
  - Multiple PPPoE sessions
  - PPTP connection method

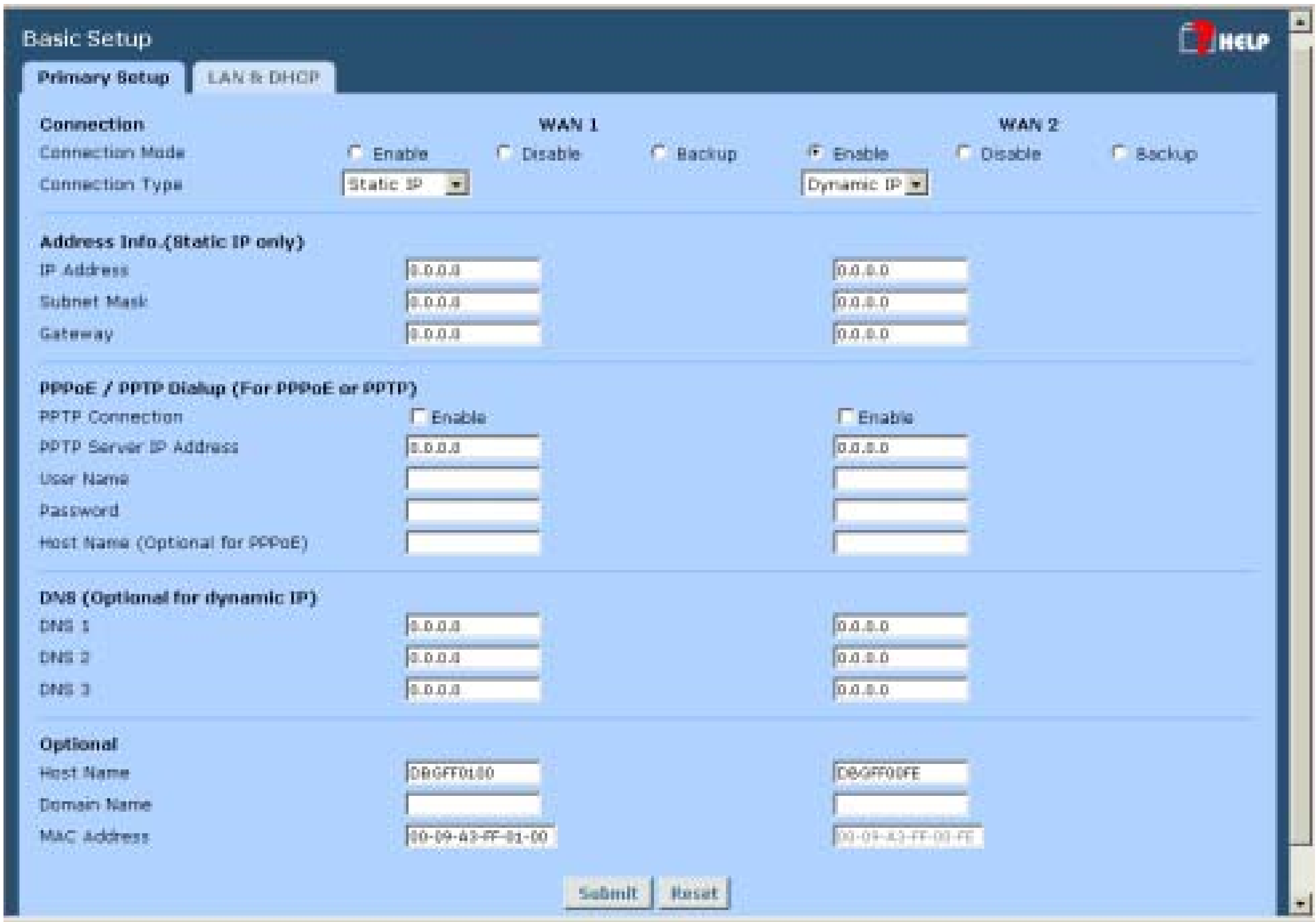


Figure 2-4: Primary Setup Screen VPN 800/2 Firewall Router

Settings – Primary Setup

Connection Mode	Select the appropriate setting: • **Enable** – Select this if you have connected a broadband modem to this port. • **Disable** – Select this if there is no broadband modem connected to this port. • **Backup** – Use this if you have a broadband modem on each port, and wish to normally use only one. Select *Enable* for the primary port, and *Backup* for the secondary port. The *Backup* port will only be used if the primary port fails.

Connection Type	Check the data supplied by your ISP, and select the appropriate option. • **Static IP** – Select this if your ISP has provided a Fixed or Static IP address. Then enter the data into the *Address Info* fields. • **Dynamic IP** – Select this if your ISP provides an IP address automatically, when you connect. You can ignore the *Address Info* fields. • **PPPoE** – Select this if your ISP uses this method. (Usually, your ISP will provide some PPPoE software. This software is no longer required, and should not be used.) If this method is selected, you must complete the *PPPoE dialup* fields. **Note:** If using the PPTP connection method, select *Static IP* or *Dynamic IP*, as appropriate, according to the IP address method used by your ISP.
Address Info	This is for *Static IP* users only. Enter the address information provided by your ISP. If your ISP provided multiple IP address, you can use the ***Multi-DMZ*** screen to assign the additional IP addresses.
PPPoE / PPTP Dialup	This is for *PPPoE* and *PPTP* users only. • Enter the *Username* and *Password* provided by your ISP. • If using PPTP, enable the *PPTP Connection* checkbox, and enter the IP address of the PPTP server. • Host name (Optional For PPPoE),This field is used by a Host to uniquely associate an access concentrator to a particular Host request. **Note:** There are additional PPPoE/PPTP options on the ***Port Options*** screen. To use multiple PPPoE sessions on either port, configure the ***Advanced PPPoE*** screen.
DNS	If using a *Fixed IP* address, you MUST enter at least 1 DNS address. If using *Dynamic IP* or *PPPoE*, DNS information is optional.
Optional	• **Host name** – This is required by some ISPs. If your ISP provided a Host Name, enter it here. Otherwise, you can use the default value. • **Domain name** – This is required by some ISPs. If your ISP provided a Domain Name, enter it here. Otherwise, you can use the default value. • **MAC address** – Some ISP's record your MAC address (also called "Physical address" or "Network Adapter address"). If so, you can enter the MAC address expected by your ISP in this field. Otherwise, this should be left at the default value.

Setup of the HotBrick VPN 800/2 Firewall Router is now complete. PCs on your LAN must now be configured. See the following section for details.

4: Configure PCs on your LAN

Overview

For each PC, the following may need to be configured:

- TCP/IP network settings
- Internet Access configuration

TCP/IP Settings

If using the default VPN 800/2 Firewall Router settings, and the default Windows 95/98/ME/2000/XP TCP/IP settings, no changes need to be made. Just start (or restart) your PC.

- By default, the VPN 800/2 Firewall Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client. In Windows, this is called *Obtain an IP address automatically*.
  Just start (or restart) your PC and it will obtain an IP address from the VPN 800/2 Firewall Router.
- If using fixed IP addresses on your LAN, or you wish to check your TCP/IP settings, refer to ***Appendix B – Windows TCP/IP Setup***.

Internet Access

To configure your PCs to use the VPN 800/2 Firewall Router for Internet access, follow this procedure:

For Windows 9x/2000

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click *Next*.
4. Select "I connect through a local area network (LAN)" and click *Next*.
5. Ensure all of the boxes on the following *Local area network Internet Configuration* screen are **unchecked**.
6. Check the "No" option when prompted "Do you want to set up an Internet mail account now?".
7. Click *Finish* to close the Internet Connection Wizard.
   Setup is now completed.

For Windows XP

1. Select Start Menu - Control Panel - Network and Internet Connections.
2. Select *Set up or change your Internet Connection*.
3. Select the *Connection* tab, and click the *Setup* button.
4. Cancel the pop-up "Location Information" screen.
5. Click *Next* on the "New Connection Wizard" screen.
6. Select "Connect to the Internet" and click *Next*.

7. Select "Set up my connection manually" and click *Next*.
8. Check "Connect using a broadband connection that is always on" and click *Next*.
9. Click *Finish* to close the New Connection Wizard.
   Setup is now completed.

Accessing AOL

To access AOL (America On Line) through the VPN 800/2 Firewall Router, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "VPN 800/2 Firewall Router".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "VPN 800/2 Firewall Router" location.

Macintosh Clients

From your Macintosh, you can access the Internet via the VPN 800/2 Firewall Router. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the required changes are:

- Set the *Router Address* field to the VPN 800/2 Firewall Router IP Address.
- Ensure your *DNS* settings are correct.

Linux Clients

To access the Internet via the VPN 800/2 Firewall Router, it is only necessary to set the VPN 800/2 Firewall Router as the "Gateway", and ensure your *Name Server* settings are correct.

Ensure you are logged in as "root" before attempting any changes.

Fixed IP Address

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your *Default Gateway* to the IP Address of the VPN 800/2 Firewall Router.
- Ensure your *DNS* (Name server) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes

   Use the "Deactivate" and "Activate" buttons, if available.

   OR, restart your system.

3: Advanced Port Setup

Overview

- ***Port Options*** contains some options, which can be set on either or both WAN ports. For most situations, the default values are satisfactory.
- ***Load Balance*** screen is only functional if you are using both WAN ports. It allows you to determine the proportion of WAN traffic sent through each port.
- ***Advanced PPPoE*** setup is required if you wish to use multiple sessions on one or both of the WAN ports. It can also be used to manually connect or disconnect a PPPoE session. Otherwise, this screen can be ignored.
- ***Advanced PPTP*** setup is required if using the PPTP connection method.

Port Options

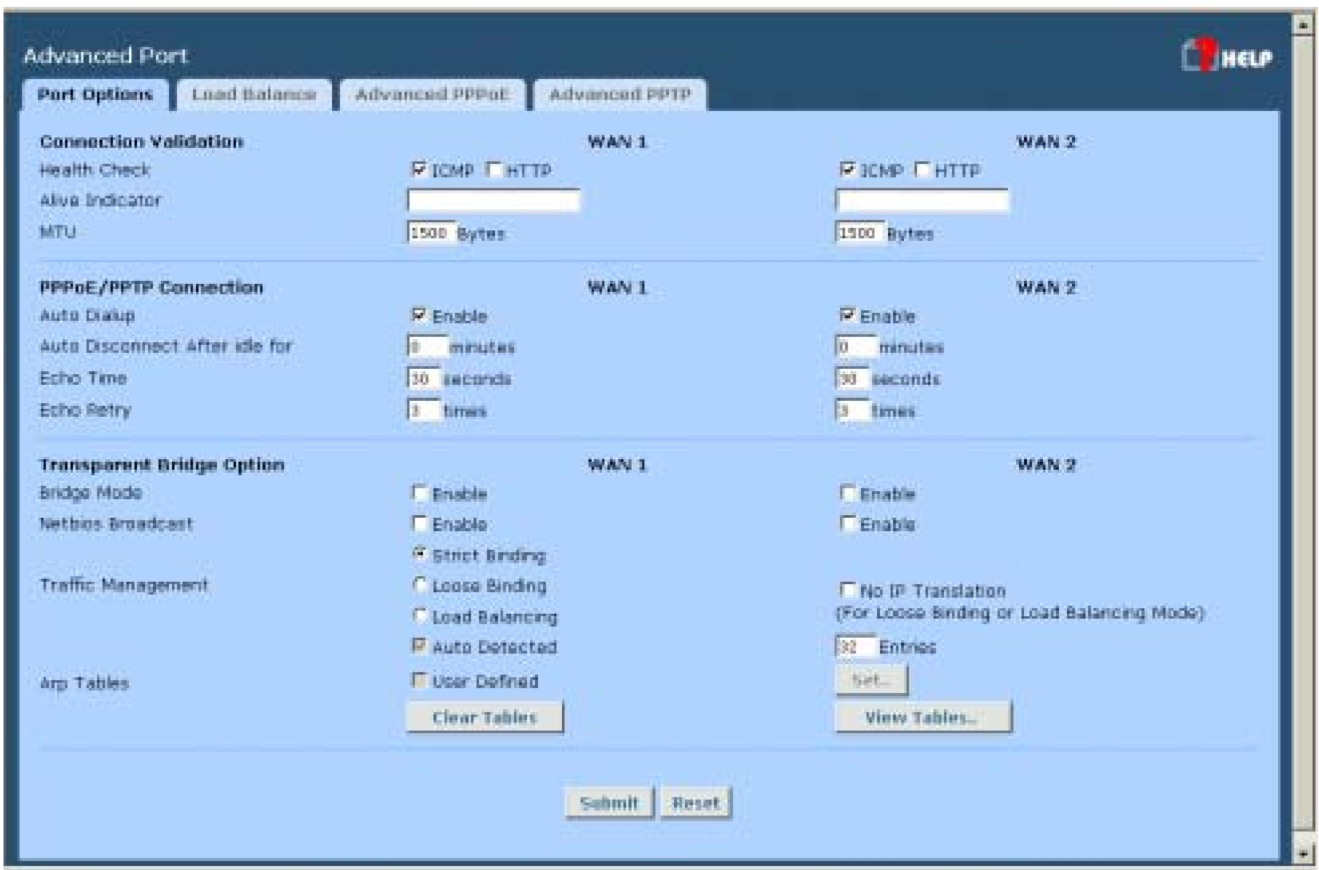


Figure 3-1: Port Options

Settings – Port Options

Connection Validation	• **Health Check** – Disable will not do Alive Indicator Check. By default health check is enable. Health checking is performing an ICMP echo request and HTTP packets to the specific destination that could be either: 1. Name or IP Address user specified in the "Alive Indicator" input box or gateway of WAN interface if "Alive Indicator" input box is left blank. • **Alive Indicator** – This is the IP address used to check if the WAN connection is operating. The VPN 800/2 Firewall Router will contact this system to check if the WAN connection is working. Change this address if you wish. Default is the gateway IP. **Note**: This is not used for PPPoE connections. • **MTU** – The Maximum Transmission Unit is used when determining the packet size to be used on the WAN interface. Normally, this does not need to be changed, but if your ISP advises you to use a particular MTU, enter it here.
PPPoE / PPTP Connection Options	• **Auto Dialup** – If set to *Enable* a connection will be established whenever outgoing WAN traffic is detected. If not Enabled, you must establish a connection manually. • **Auto Disconnect** – This determines when an idle connection will be terminated. Enter the required time period. • **Echo Time** – This determines how often an Echo request is sent to the PPPoE server. The Echo request is used to determine if the connection is still valid. Normally, there is no need to change the default value. • **Echo Retry** – The number of time the Echo request will be sent, if there is no response to the first request. Normally, there is no need to change the default value.
Transparent Bridge Option	• **Bridge Mode** – If set to Enable, this WAN port doesn't use NAT & Load Balance function when LAN/WAN IP have the real IP addresses on the same network segment. • **NetBIOS Broadcast** – This function can allow you access files through Microsoft network neighborhood. If you enable the NetBIOS Broadcast function. • **Traffic Management** –**Strict Binding:** traffic from bridge hosts(eg. transparent to wan1) can only go thru that specified wan(eg. wan1) interface. **Loose Binding:** Traffic from bridge hosts (eg. transparent to wan1) can go thru alternative wan(eg. wan2) interface when bind interface (eg. wan1) is down, it's acting like a fail over mechanism for transparent bridge mode. **Load Balancing:** Traffic from bridge hosts (eg. transparent to wan1) can go thru either wan(eg. wan1 or wan2) interface based on loading mechanism specified in the load balance section, it's acting like a load balancing mechanism for transparent bridge mode. • **ARP Table –** ARP table is used by the device to determine the bridge hosts' location (eg, inside/outside wan and which wan) its' size can be adjusted if needed.

Load Balance

This screen is only operational if using Internet connections on both WAN ports.



Figure 3-2: Load Balance

These settings are only functional if using both WAN ports. If using both WAN ports, these settings determine the proportion of traffic sent over each port.

Settings – Load Balance

Load Balance Configuration	• **Enable** – Use this to enable your Load Balance settings. Unless this is checked, the other settings on this screen have no effect. • **Balance Type** – Select the desired option: • Bytes rx+tx – Traffic is measured by Bytes. • Packets rx+tx – Traffic is measured by Packets. • Sessions established – Traffic is measured by Sessions. • IP Address – Traffic is measured by IP Address. • **Loading Share on WAN 1** – Enter the percentage (%) of traffic to be sent over WAN 1. If one WAN port connection has greater bandwidth than the other, the one with the greater bandwidth should be given a higher percentage of traffic than the other. Click the "Update" button to save your changes.
NAT Statistics	This section displays the current data about WAN 1 and WAN 2. You can use this information to help you "fine-tune" the settings above.
Interface Statistics	This section displays cumulative statistics. Use the "Restart Counters" button to restart these counters when required.
Buttons	• **Update** – Save the settings on this screen. • **Refresh** – Update the data on screen. • **Restart Counters** – Restart the counters used in the "Interface Statistics" section.

Advanced PPPoE

The screen is required in order to use multiple PPPoE sessions on the same WAN port.

It can also be used to manually connect or disconnect a PPPoE session.



Figure 3-3: Advanced PPPoE

Settings – Advanced PPPoE

Select WAN Port & Session	Select the desired WAN Port and Session, then click the "Select" button. The data for the selected Port/Session will then be displayed in the *WAN IP Account* section. **Session MTU** - The Maximum Transfer Unit for PPPoE packets data. Leave it as default, unless the ISP offers different PPPoE packets data size.
WAN IP Account	• **User Name** – Enter the PPPoE user name assigned by your ISP. • **Password** – Enter the PPPoE password assigned by your ISP. • **Verify Password** – Re-enter the PPPoE password assigned by your ISP. • **IP Address** – If you have a fixed IP address, enter if here. Otherwise, this field should be left at 0.0.0.0. • **Host Name** – This field is used by a Host to uniquely associate an access concentrator to a particular Host request.

Action	Use the "Connect" and "Disconnect" buttons to establish or terminate a connection on this session, if required.
Connection Status	This displays the current connection status for each session.

Advanced PPTP

This screen is only useful if using the PPTP connection method.

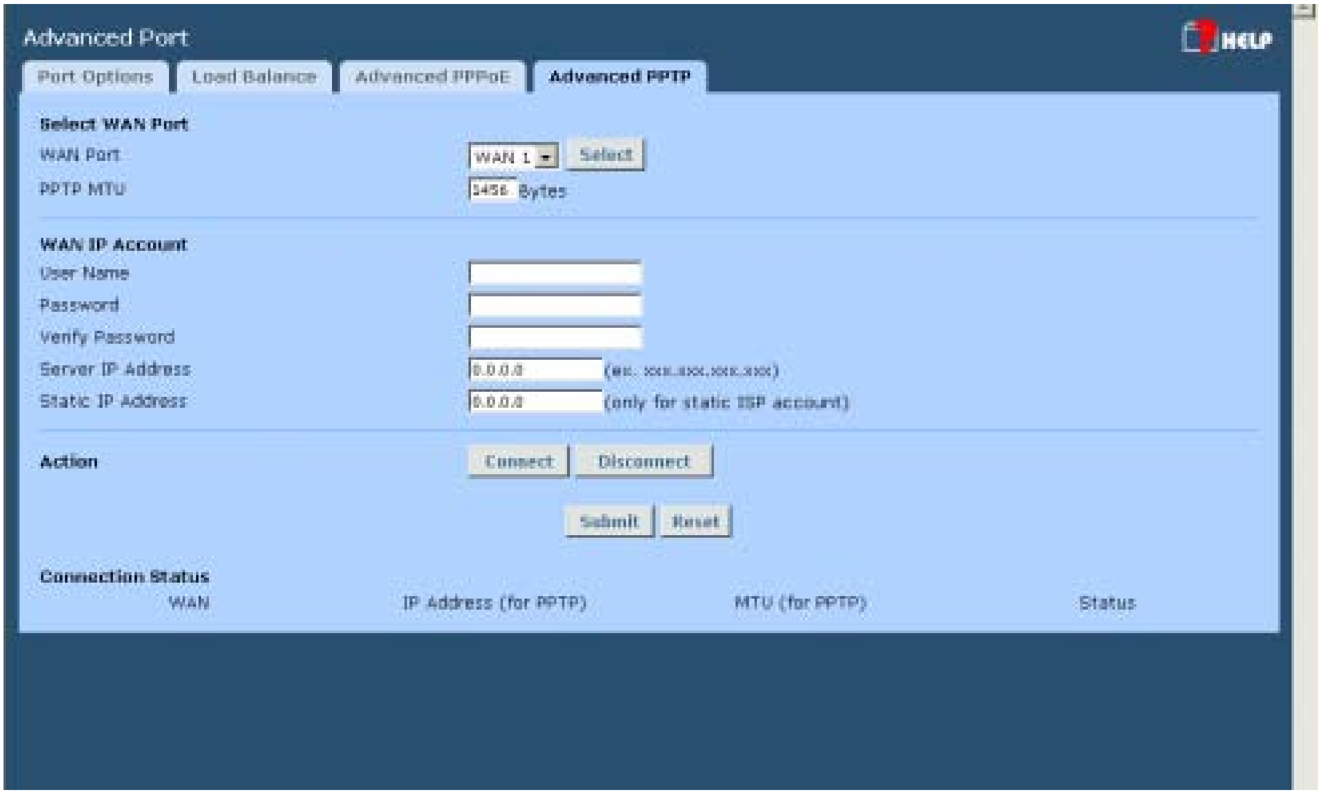


Figure 3-4: Advanced PPTP

Settings – Advanced PPTP

Select WAN Port	Select the desired Port, and then click the "Select" button. The data for the selected Port will then be displayed in the *WAN IP Account* section. **PPTP MTU** – Maximum transfer unit for PPTP. The default value is 1456.
WAN IP Account	• **User Name** – The PPTP user name (login name) assigned by your ISP. • **Password** – The PPTP password associated with the *User Name* above. This is assigned by your ISP, and used to login to the PPTP Server. • **Verify Password** – Re-enter the PPTP password assigned by your ISP. • **Server IP Address** – Enter the IP address of the PPTP Server, as provided by your ISP. • **Static IP Address** – If you have a fixed IP address, enter if here. Otherwise, this field should be left at 0.0.0.0.
Action	Use the "Connect" and "Disconnect" buttons to establish or terminate a connection on this session, if required.
Connection Status	This displays the current connection status.

4: Advanced Setup

Overview

The following advanced features are provided.

- Host IP Setup
- Virtual Servers
- Custom Virtual Server
- Special Applications
- Dynamic DNS
- Multi DMZ
- Advanced Features
- UpnP
- NAT Setting

This chapter contains details of the configuration and use of each of these features.

Host IP Setup

This feature is used in the following situations:

- You have Multi-Session PPPoE, and wish to bind each session to a particular PC on your LAN.
- You wish to use the ***Access Filter*** feature. This requires that each PC be identified by using the ***Host IP Setup*** screen.
- You wish to have different ***Block URL*** settings for different PCs. This requires that each PC be identified by using the ***Host IP Setup*** screen. (You do not have to use the Host IP feature to apply the same ***Block URL*** settings to all PCs.)
- You wish to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this "Obtain an IP address automatically") while gaining the benefits of a fixed IP address. The PC's IP address will never change, so it can be provided to other people and applications.

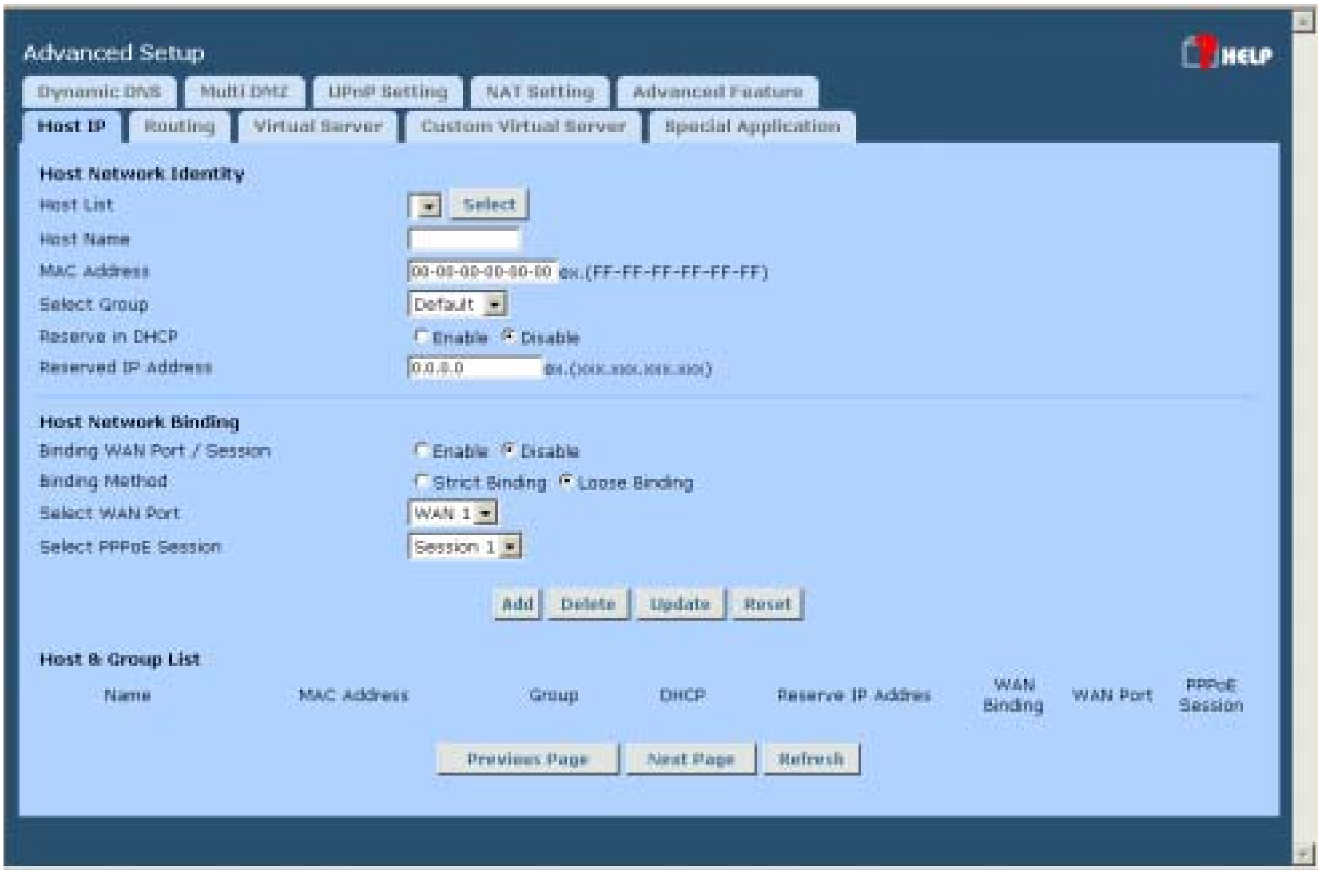


Figure 4-1: Host IP Setup

Settings – Host IP Setup

Host Network Identity	This section identifies each Host (PC) • **Host List** – When adding a new Host, ignore this list. To edit an existing entry, select it from the list, and click the "Select" button. The data fields will then be updated with data for the selected entry. • **Host name** – Enter a suitable name. Generally, you should use the "Hostname" (computer name) defined on the Host itself. • **MAC Address** – Also called *Physical Address* or *Network Adapter Address*. Enter the MAC address of this host. • **Select Group** – Select the group you wish to put this host into. • **Reserve in DHCP** – Select *Enable* to reserve a particular (LAN) IP address for a particular PC on your LAN. This allows the PC to use DHCP (Windows calls this "obtain an IP address automatically") while having an IP address, which never changes. • **Reserved IP** – Enter the IP address you wish to reserve, if the setting above is *Enable*. Otherwise, ignore this field.

Host Network Binding	• **Bind WAN port/Session** – Select *Enable* if you wish to associate this PC with a particular PPPoE Session. All traffic for that PC will then use the selected PPPoE port and session. • **Binding Method** – Suppose your PC is bound to WAN1 port, now you are selecting "Strict Binding". If WAN1 port is disconnected, your packets cannot go out through WAN2 port, if WAN2 port is still alive. If you are selecting "Loose Binding" then when WAN1 port is disconnected, your packets will automatically go to WAN2, if WAN2 is alive. • **Select WAN Port/Select PPPoE session** – If the setting above is *Enable*, select the desired Port and Session. Otherwise, ignore these settings. **Note**: Multiple PPPoE sessions are defined on the ***Advanced PPPoE*** screen.
Buttons	• **Add** – Use this to add a new entry to the database, using the data shown on screen. • **Delete** – Click this to delete the selected entry. • **Update** – Use this to update the selected entry, after making the desired changes. • **Reset** – Reverse any changes you have made since loading the data from the VPN 800/2 Firewall Router.
Host & Group List	This table shows the current bindings.

Virtual Servers

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server's IP address is only valid on your LAN, not on the Internet.
- Attempts to connect to devices on your LAN are blocked by the firewall in the VPN 800/2 Firewall Router.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

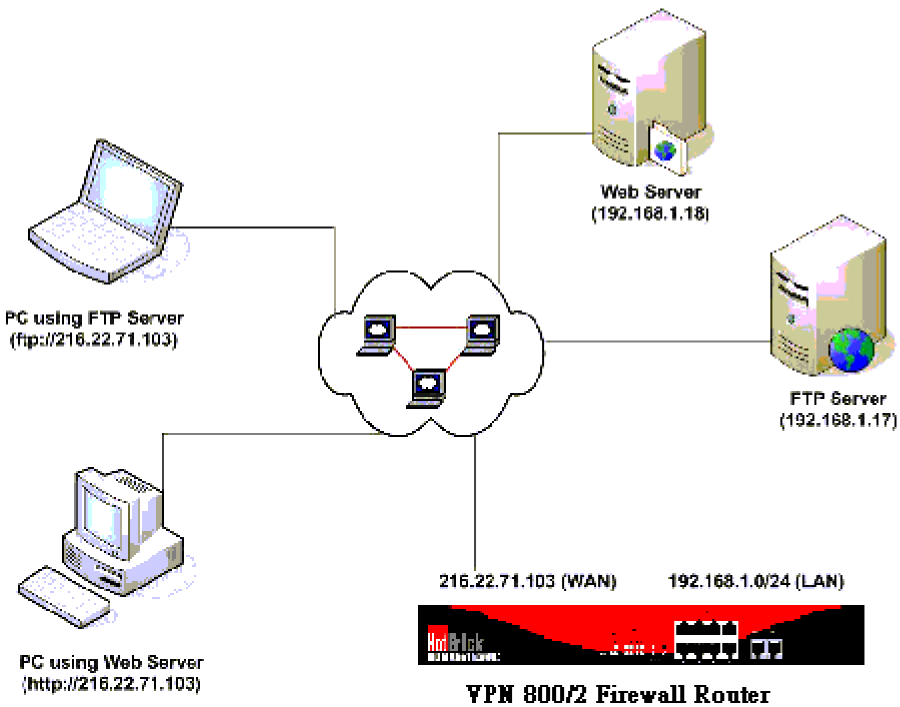


Figure 4-2: Virtual Servers

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the VPN 800/2 Firewall Router's Internet IP Address (the IP Address allocated by your ISP).
e.g.

```
http://205.20.45.34
ftp://205.20.45.34
```

- To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

- This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. However, you can use the *Dynamic DNS* feature (explained later in this chapter) to allow users to connect to your Virtual Servers using a URL, instead of an IP Address.
  e.g.
  `HTTP://my_domain_name.dyndns.org`
  `FTP://my_domain_name.dyndns.org`



Figure 4-3: Virtual Server

Settings – Virtual Server

Virtual Server	**Enable** - Use this to Enable or Disable each Virtual server as required.
	Server Type - Select the desired Server type. If the type of Server you wish to use is not listed, use the ***Custom Virtual Server*** screen to define your own type.
	LAN IP Address - Enter the IP address of the PC on your LAN which is running the required Server software. Each PC should have a fixed IP address, or have a reserved IP address. (See the ***Host IP*** section earlier in this chapter for details on reserving an IP address.)

Custom Virtual Servers

This screen allows you to define your own Server types, for situations when the desired Server type is not listed on the ***Virtual Servers*** screen.

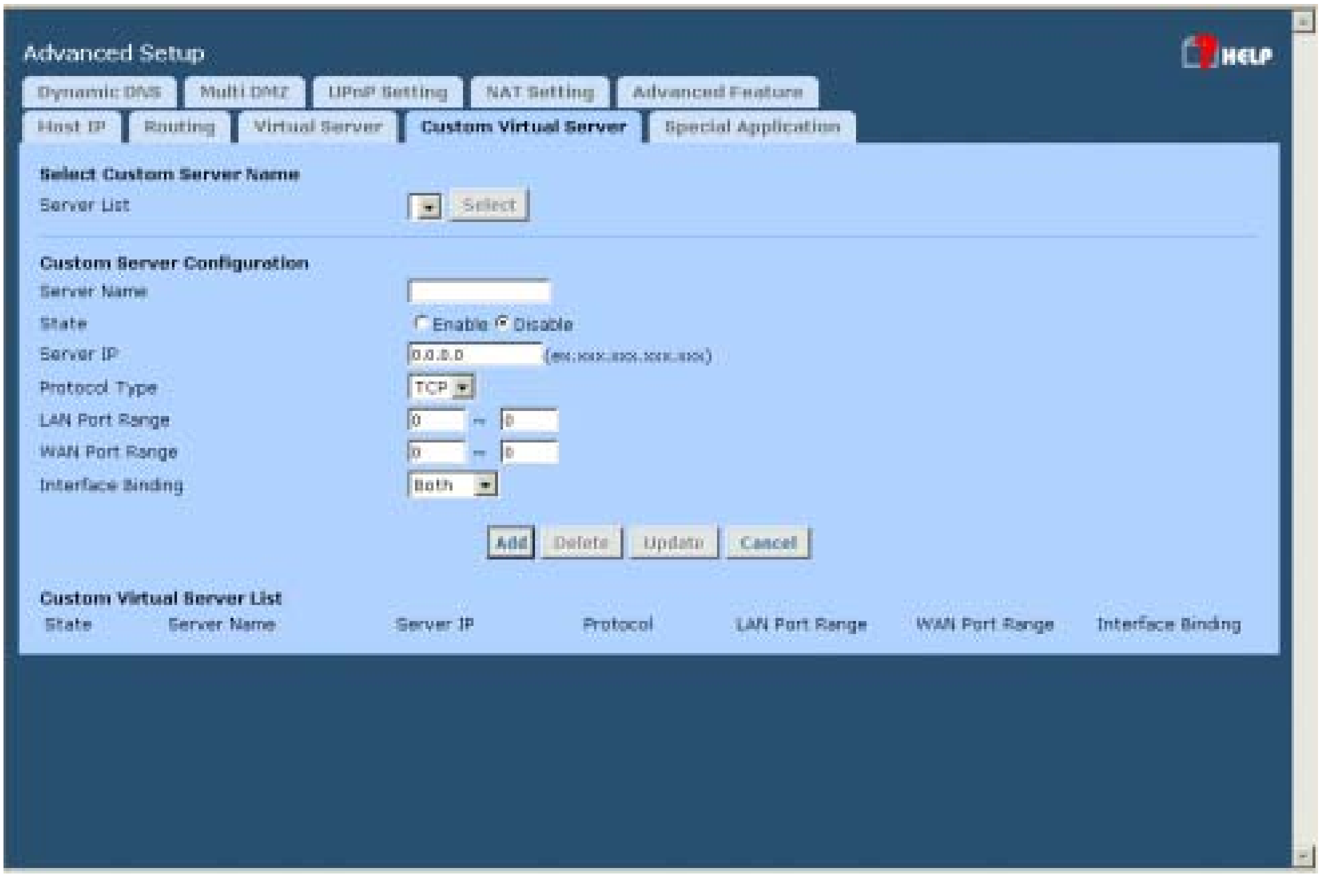


Figure 4-4:Custom Virtual Servers

Settings – Custom Virtual Servers

Select Custom Server Name	**Server List** If creating a new entry, ignore this list. To edit an existing entry, select it, and then click the "Select" button. The screen will update with data for the selected entry.
Custom Server Configuration	This data defines the Custom Virtual Server: • **Server Name** – Enter a suitable name for this server. • **State** – Use this to Enable or Disable the server as required. • **Server IP** – Enter the IP address of the PC on you LAN which is running the required Server software. Each PC should have a fixed IP address, or have a reserved IP address. (See the ***Host IP*** section earlier in this Chapter for details on reserving an IP address.)

	Each PC must be running the appropriate Server software. • **Protocol Type** – Select the network protocol used by this sever type. • **LAN Port Range** – Enter the range of port number used for outgoing traffic from this Server. If only a single port is required, enter it in both fields. • **WAN Port Range** - – Enter the range of port number used for incoming traffic to this Server. If only a single port is required, enter it in both fields • **Interface Binding** – This selection allows severs binding WAN1 port or WAN2 port, or even both WAN1 and WAN2 ports together.
Buttons	• **Add** – Create a new Special Application entry. • **Delete** – Delete the selected entry. • **Update** – Save any changes you have made to the current entry. • **Cancel** – Cancel any changes you have made since the last save operation.
Custom Virtual Server List	This table shows details of all Custom Virtual Servers which have been defined.

Special Applications

If you use Internet applications which have non-standard connections or port numbers, you may find that they do not function correctly because they are blocked by the firewall in the Load Balancer. In this case, you can define the application as a "Special Application" in order to make it work.

Note that the terms "Incoming" and "Outgoing" on this screen refer to traffic from the client (PC) viewpoint

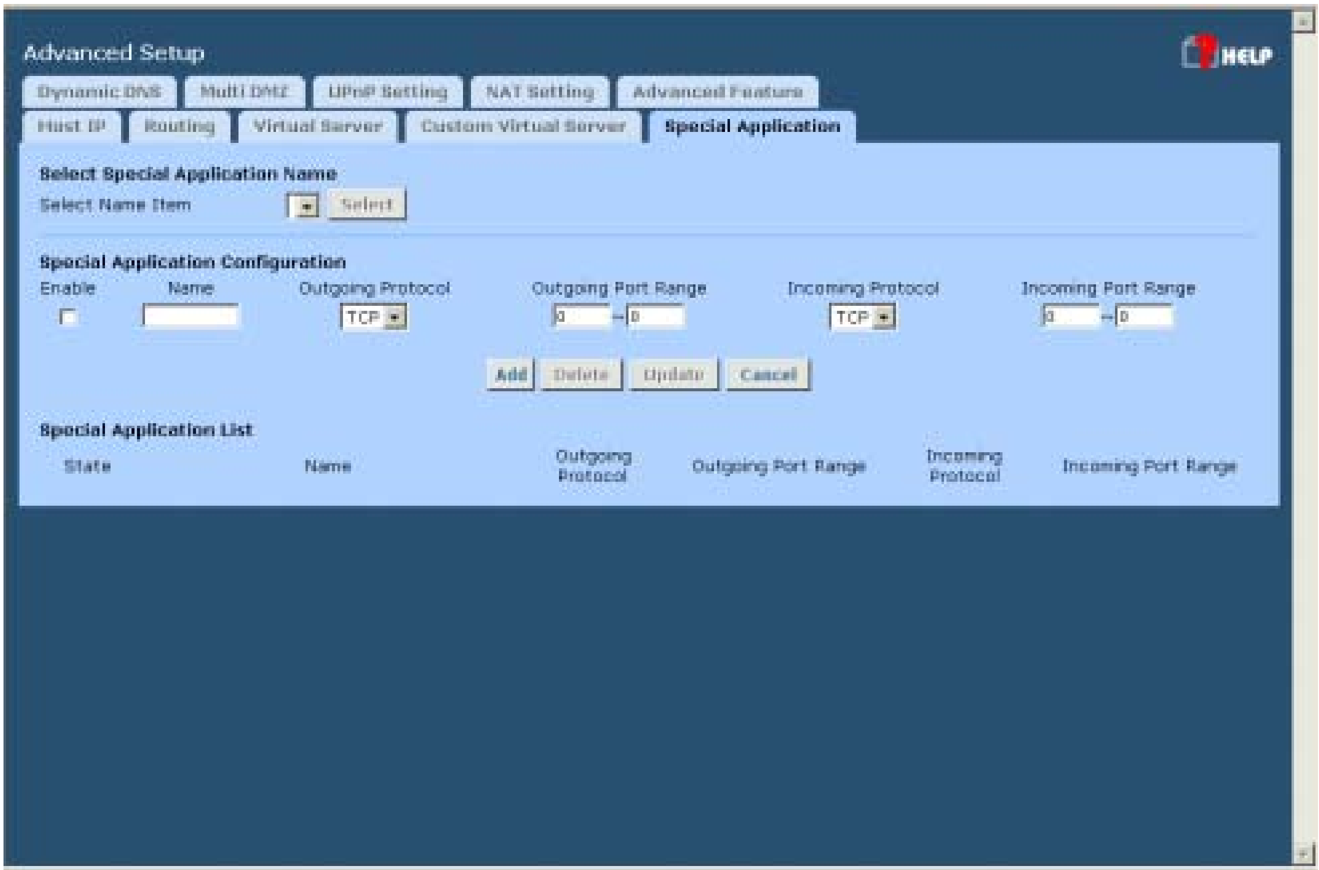


Figure 4-5: Special Applications

Settings – Special Applications

Select Special Application Name	**Select Name Item** - This lists any special applications, which are currently defined. • If adding a new Special Application, ignore this list. Just enter your data in the *Special Application Configuration* section, and click the "Add" button. • To edit an existing entry, select it from this list, and click the "Select" button. The data for the selected application will then be displayed in the *Special Application Configuration* section. Make any required changes, and then click the "Update" button.

Special Application Configuration	**Enable** - Use this to Enable or Disable this Special Application as required. **Name** - Enter a descriptive name to identify this Special Application. **Outgoing Protocol** - Select the protocol used by this application, when sending data to the remote server or PC. **Outgoing Port Range** - Enter the beginning and end of the range of port numbers used by the application server, for data you send. If the application uses a single port number, enter it in both fields. **Incoming Protocol** - Select the protocol used by this application, when receiving data from the remote server or PC. **Incoming Port Range** - Enter the beginning and end of the range of port numbers used by the application server, for data you receive. If the application uses a single port number, enter it in both fields.
Buttons	**Add** – Create a new Special Application entry. **Delete** – Delete the selected entry. **Update** – Save any changes you have made to the current entry. **Cancel** – Cancel any changes you have made since the last save operation.
Special Application List	This shows details of all Special Applications which are currently defined.

Using a Special Application on your PC

- Once the *Special Applications* screen is configured correctly, you can use the application on your PC normally. Remember that only one (1) PC can use each Special application at any time.
- Also, when 1 PC is finished using a particular Special Application, there may need to be a "Time-out" period before another PC can use the same Special Application.
- If an application still cannot function correctly, try using the "DMZ" feature, if possible.

Dynamic DNS

Dynamic DNS is very useful when combined with the *Virtual Server* feature. It allows Internet users to connect to your Virtual Servers using a URL, rather than an IP Address.

This also solves the problem of having a dynamic IP address. With a dynamic IP address, your IP address may change whenever you connect to your ISP, which makes it difficult to connect to you.

You must register for the Dynamic DNS service. The VPN 800/2 Firewall Router supports 4 types of service providers:

- Hotbrick dynamic DNS is available at: http://www.hotbrick.dns4biz.com/hotbrick.php3
- TZO at http://www.tzo.com
- 3322 is available in China at http://www.3322.org
- Standard client, available at http://www.dyndns.org
  Other sites may offer the same service, but can not be guaranteed to work.

To use the Dynamic DNS feature

1. Register for the service from your preferred service provider.
2. Follow the service provider's procedure to have a Domain Name (Host name) allocated to you.
3. Configure the ***Dynamic DNS*** screen, as described below.
4. The VPN 800/2 Firewall Router will then automatically update your IP Address recorded by the Dynamic DNS service provider.
5. From the Internet, users will now be able to connect to your Virtual Servers (or DMZ PC) using your Domain name.

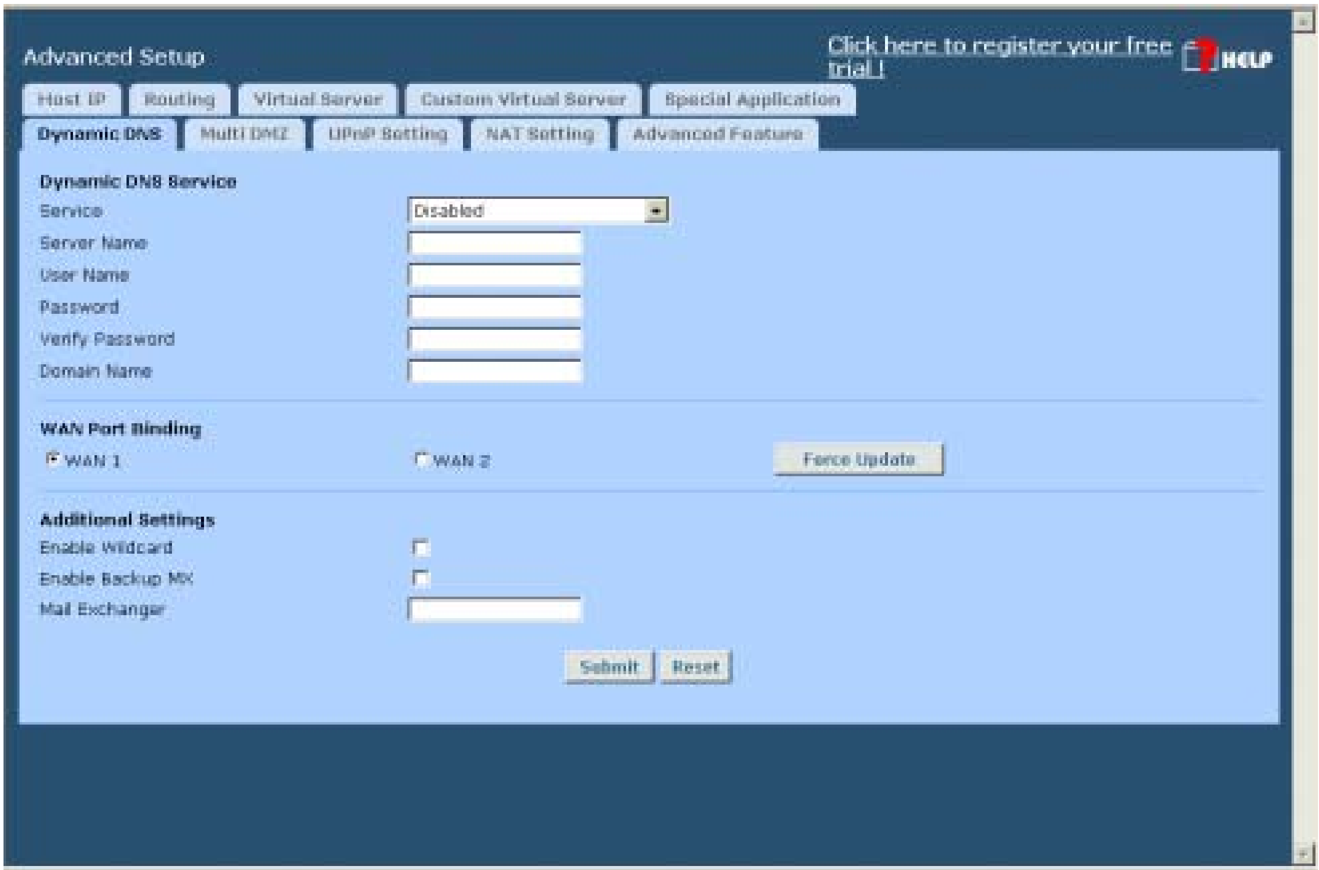


Figure 4-6: Dynamic DNS

Settings – Dynamic DNS

Dynamic DNS Service	Use this to Enable/Disable the Dynamic DNS feature, and select the required service provider. • **Disable** – Dynamic DNS is not used. • **DNS4BIZ Hotbrick Premium** – It provides reliability for normal business requirement. • **DNS4BIZ Hotbrick Business** – Designed for VPN connections & mission critical applications your DNS service is hosted on dedicated high-end servers with 24/7 Monitoring to ensure the highest possible availability & reliability. • **TZO** – Select this to use the TZO service (www.tzo.com). You must configure the *TZO* section of this screen. • **Standard Client** – Select this to use the standard service (from www.dyndns.org or other provider). You must configure the *Standard Client* section of this screen. • **3322(in China)** – This is available in China. It is similar to “Standard client” • **User Defined DDNS Server** – This is the user define DDNS server. If the DDNS other than TZO, dyndns.org and 3322.

WAN Port Binding	• Select the WAN port on which the Dynamic DNS is used. • The "Force Update" button will update your record on the Dynamic DNS Server immediately.
Additional Setting	These options are available if using the standard client. • **Enable Wildcard** – If selected, traffic sent to sub-domains (of your Domain name) will also be forwarded to you. • **Enable backup MX** – If enabled, you must enter the *Mail Exchanger* address below. • **Mail Exchanger** – If the setting above is enabled, enter the address of the backup Mail Exchanger.

Multi DMZ

This feature allows each WAN port IP address to be associated with one (1) computer on your LAN. All outgoing traffic from that PC will be associated with that WAN port IP address. Any traffic sent to that IP address will be forwarded to the specified PC, allowing unrestricted 2-way communication between the "DMZ PC" and other Internet users or Servers.

Note:

The "DMZ PC" is effectively outside the Firewall, making it more vulnerable to attacks. For this reason, you should only enable the DMZ feature when required

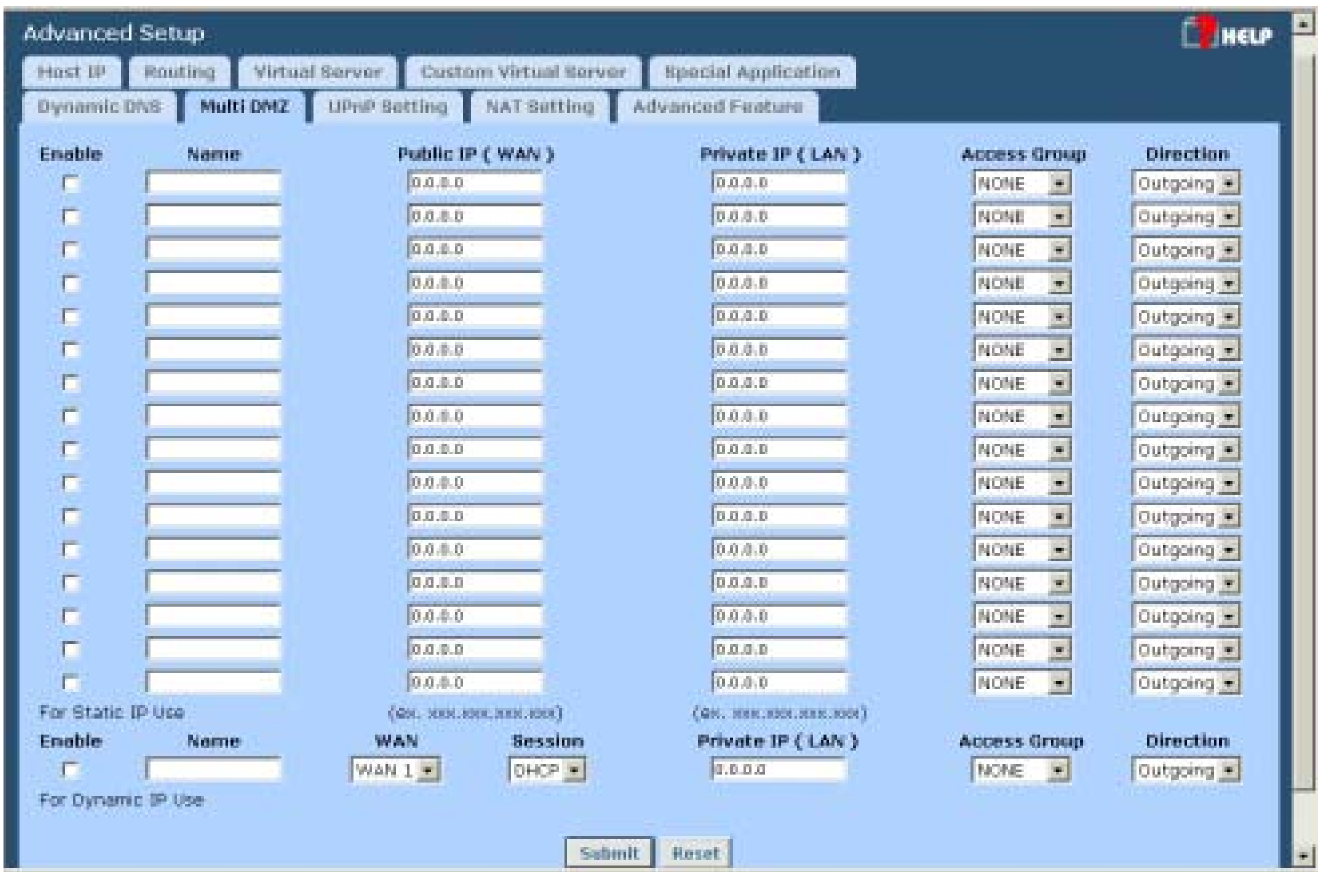


Figure 4-7: Multi DMZ

Settings – Multi DMZ

Enable	Use this to enable or disable the DMZ setting, as required.
Name	Enter a name to assist you to remember this setting. This name has no effect on the operation.
For Static IP	
Public IP address	Enter the WAN port (Internet) IP address you wish to associate to a PC. This IP address must have been allocated to you by your ISP.
Private IP Address (LAN)	Enter the IP address of the PC you wish to associate with this WAN port IP address. This IP address should be fixed, or reserved. (See the ***Host IP*** section for details on reserving an IP address.)
For Dynamic IP	
WAN	Select the desired WAN port.
Session	• Select "DHCP" if the IP address on this WAN port is dynamically assigned. You can only select assign one (1) Private (LAN) IP address to each port. • If using multi-session PPPoE, select the desired PPPoE session. These sessions are defined on the ***Advanced PPPoE*** screen. You can assign one (1) one (1) Private (LAN) IP address to each PPPoE session.
Private IP Address (LAN)	Enter the IP address of the PC you wish to associate with this WAN port IP address. This IP address should be fixed, or reserved. (See the ***Host IP*** section for details on reserving an IP address.)
Access Group	You can decide the users to have the authority of using DMZ, by define the groups.
Direction	For DMZ, you can allow inbound, outbound only, or both inbound and outbound both.

UPnP

With UPNP (Universal Plug & Play) function, it can easily setup and configure an entire network, enable discovery and control of networked devices and services.

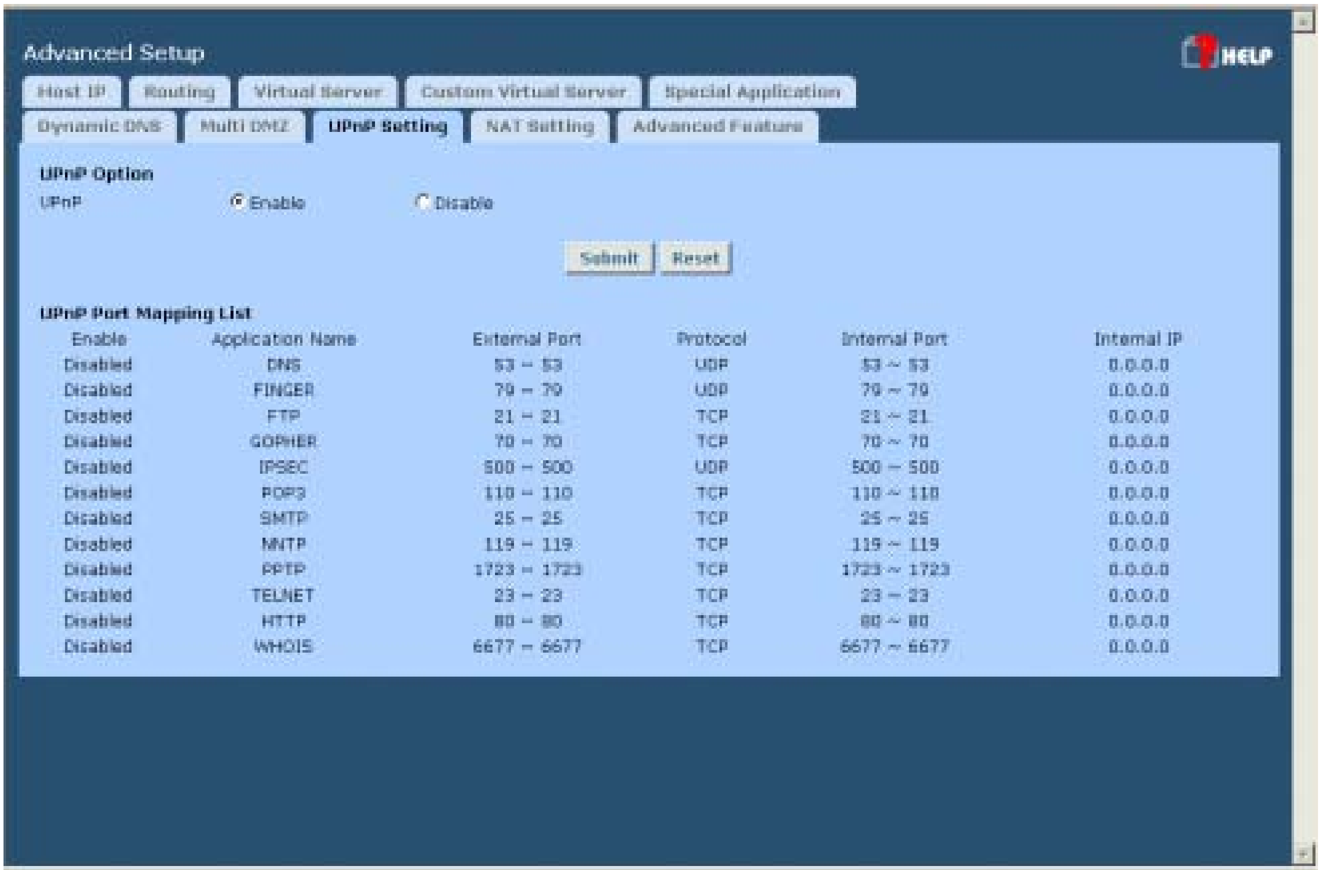


Figure 4-8: UPnP

Settings – UPnP

UPnP Option	If you Enable UPnP, then this two wan router will become one of the entire local network. You can find out there is an icon show up on network neighborhood on the window XP OS. Every time you add a new network device with port mapping, The new network device will appear on the mapping list.

NAT Setting

NAT (Network Address Translation) is the technology which allows one (1) WAN (Internet) IP address to be used by many LAN users.

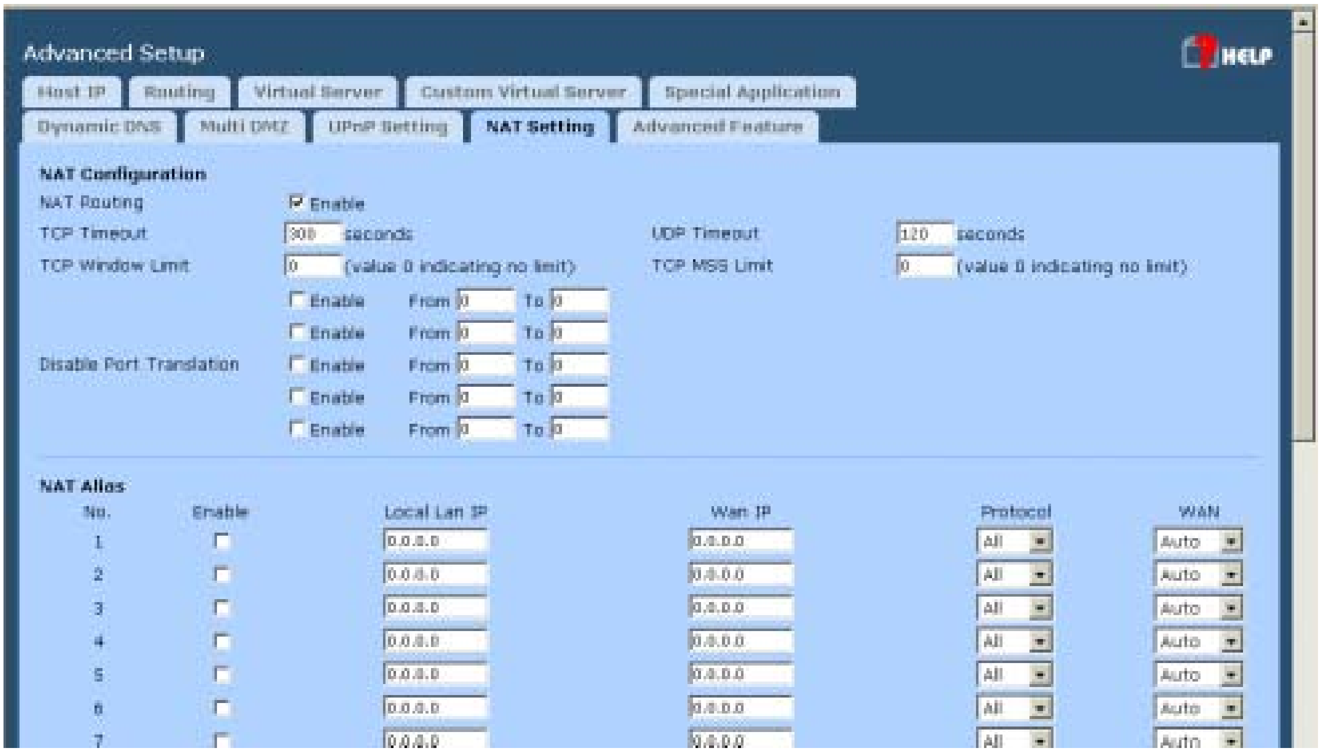


Figure 4-9: NAT

Settings – NAT

NAT Configuration	• **NAT Routing** – You can enable or disable NAT through the check box. If you disable NAT checkbox, it will act as a bridge or Static Router. Most features will be unavailable. • **TCP Timeout** – Enter the desired value to use on both WAN ports. The default is 300. • **UDP Timeout** – Enter the desired value to use on both WAN ports. The default is 120. • **TCP Window Limit** – Enter the desired value to use on both WAN ports. The default is 0 (no limit). • **TCP MSS Limit** – Enter the required MSS (Maximum Segment Size) to use on both WAN ports. The default is 0 (no limit)., • **Disable Port Translation** –If some packets whose port number cannot be translated for special applications, you must input value in port range for **"**Disable Port Translation"
NAT Alias	• For each alias entry, the Wan IP acts as an alias IP of the host with Local Lan IP to internet via the specified WAN port for the specified Protocol packets

Advanced Features

This screen allows you to change some advanced settings:

- **Remote Access Configuration** – This feature allows you to manage the VPN 800/2 Firewall Router via the Internet. You can restrict access to a specified IP address or address range.
- **External Filters Configuration** – These settings determine whether or not the VPN 800/2 Firewall Router should respond to ICMP (ping) requests received from the WAN port.
- **Interface Binding** – Use these to ensure that certain traffic is sent by a particular WAN port, and thereby a particular ISP account. These settings are only useful if using both WAN ports.
- **Protocol & Port Binding** – This allows you binding WAN1 or WAN2 ports by selecting TCP/UDP protocol.

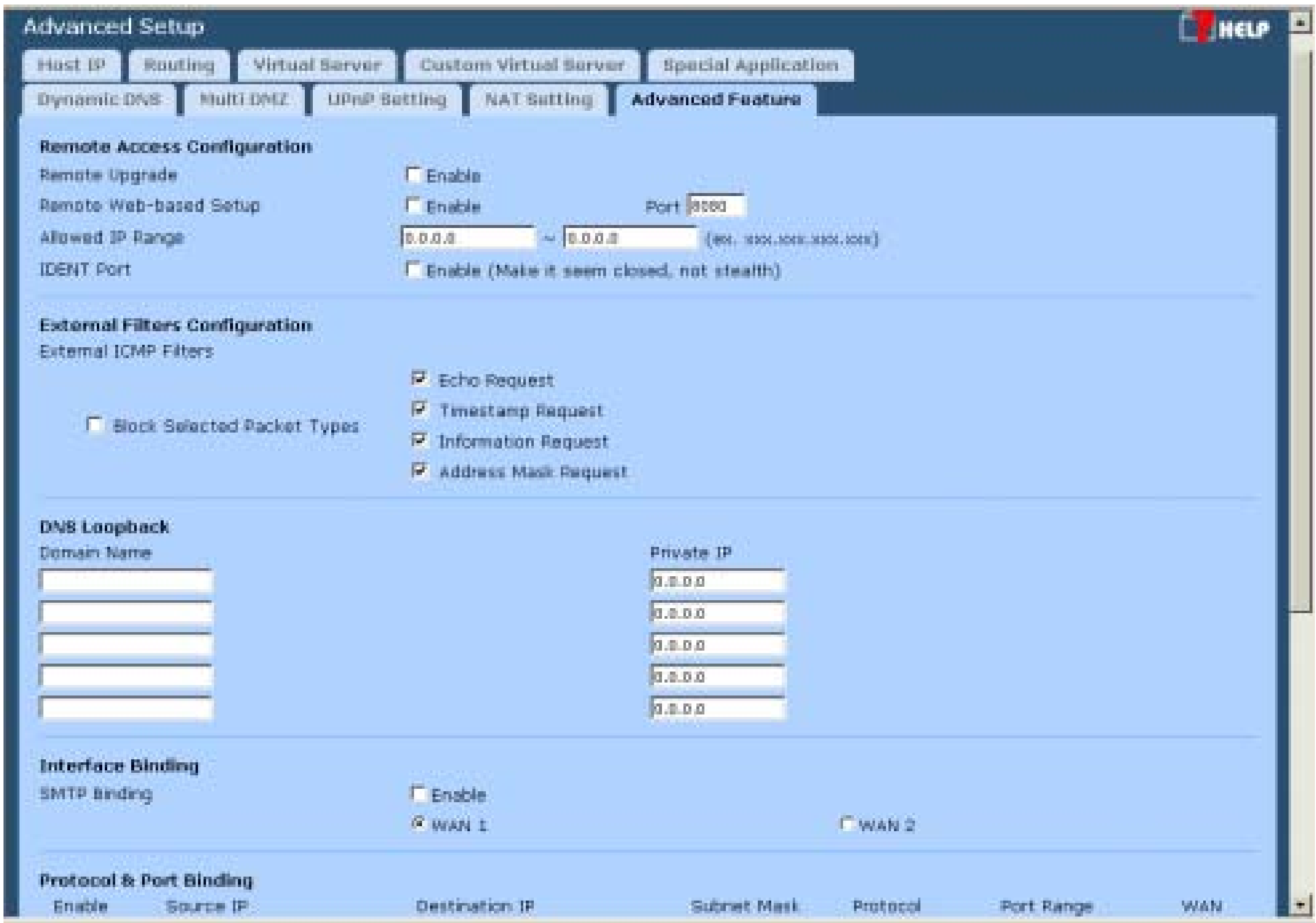


Figure 4-10: Advanced Feature

Settings – Advanced Features

Remote Access Configuration	• **Remote Upgrade** – If enabled, you can use the supplied Windows program to remotely upgrade the Firmware. If not enabled, upgrades must be performed by a PC on the LAN. • **Remote Web-based setup** - – If enabled, access to the Web-based interface is available via the Internet. (See below for details.) If not enabled, access is only available to PCs on the LAN. • **Port** – The port number used when connecting remotely. See below for details. • **Allowed IP range** – Remote access is only available to the IP addresses entered here. ◦ Leaving these fields blank will allow access by all PCs. ◦ These addresses must be Internet IP addresses, not addresses on the local LAN. ◦ To specify a single address, enter it in both fields. • **IDENT Port** – Port 113 is associated with the Internet's (Identification / Authentication) service. When a client program in your computer contacts a remote server for services such as POP, IMAP, SMTP, that remote server sends back a query to the "Ident" server running in many systems listening for these queries on port 113. This means that port 113 is often probed by attackers as a rich source of your personal information. By default it is “Disable”.
External Filters Configuration	These settings determine whether or not the VPN 800/2 Firewall Router should respond to ICMP (ping) requests received from the WAN port. • **Block Selected packet types** – This acts as "master" switch. If checked, the selected packet types are blocked. Otherwise, they are accepted. • **Echo Request, Timestamp Request, …** Select the packet types you wish to block, using the checkboxes.
DNS Loopback	When you have some servers on LAN and their domain names have already registered on public DNS. To avoid DNS loopback problem, please enter the following fields. • **Domain Name** – Enter the domain name specified by you for local host/server. • **Private IP** – Enter the private IP address of your local host/server.

Interface Binding	**SMTP (Simple Mail Transport Protocol) Binding** Unless you are using E-mail accounts from different ISPs on each port, you can ignore these settings. Some ISPs configure their E-mail Servers so they will not accept E-mail from IP addresses not allocated by themselves. If you are using accounts from different ISPs, sending E-mail over the wrong port may result in non-acceptance of the mail. In this case, you can use these settings to correct the problem. • **Enable** - If enabled, the port you specify below will be used for all outgoing SMTP traffic. If not enabled, either port will be used. • **WAN 1 / WAN 2** – Select the desired port.
Protocol & Port Binding	**Protocol and Port Binding** Use these settings if you wish to ensure that particular traffic is sent by a particular WAN port, and thereby a particular ISP account. • **Enable** - Enable or disable each item as required. • **Source IP** - IP address of source which packets are sent from. • **Destination IP** – IP address of destination which packets are sent to. • **Subnet Mask** – With subnet mask other than 255.255.255.255, you can make an IP sub-network as your destination. • **Protocol** - Select the protocol used by the traffic you wish to configure. • **Port Range** - Enter the beginning and end of the port range used by the traffic you wish to configure. If only a single port is used, enter the port number in both fields. • **WAN** - Select the port you wish this traffic to use.

Using Remote Web-based Setup

To connect to the Load Balancer from a remote PC via the Internet:

1. Ensure that both your PC and the VPN 800/2 Firewall Router are connected to the Internet.
2. Start your Web Browser.
3. In the "Address" bar, enter "HTTP://" followed by the Internet IP Address of the VPN 800/2 Firewall Router If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)
   e.g.

   `HTTP://123.123.123.123:8080`

   - This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.
   - If using the ***Dynamic DNS*** feature, you can connect using the domain name allocated to you.
     e.g.
     `HTTP://my_domain_name.dyndns.org:8080`

5: Security Management

Overview

- ***Block URL*** It can block specific website by configure IP address, URL or Key words
- ***Access filter*** You can block all Internet access or select block well-known port or block user define ports by groups.
- ***Session Limit*** It can eliminate users access Internet, and send email alert to the administrator. If the device detect new sessions that is exceed the maximum sampling time.
- ***System Filter Exception*** It can eliminate users access Internet, and send email alert to the administrator. If the device detect new sessions that is exceed the maximum sampling time.

Block URL

This feature allows you to block access to undesirable Web sites. You can block by URL, IP address, or Keyword. You can also have different blocking settings for different groups of PCs.

- In operation, every URL is searched to see if it matches or contains any of the URL or keywords entered here. Then, after a DNS lookup determines the IP address of the requested site, the site's IP address is checked against IP address entries on this screen.
- Note that a single IP address may host many Web sites. Entering the IP address on this screen will block all Web sites hosted on that IP address.

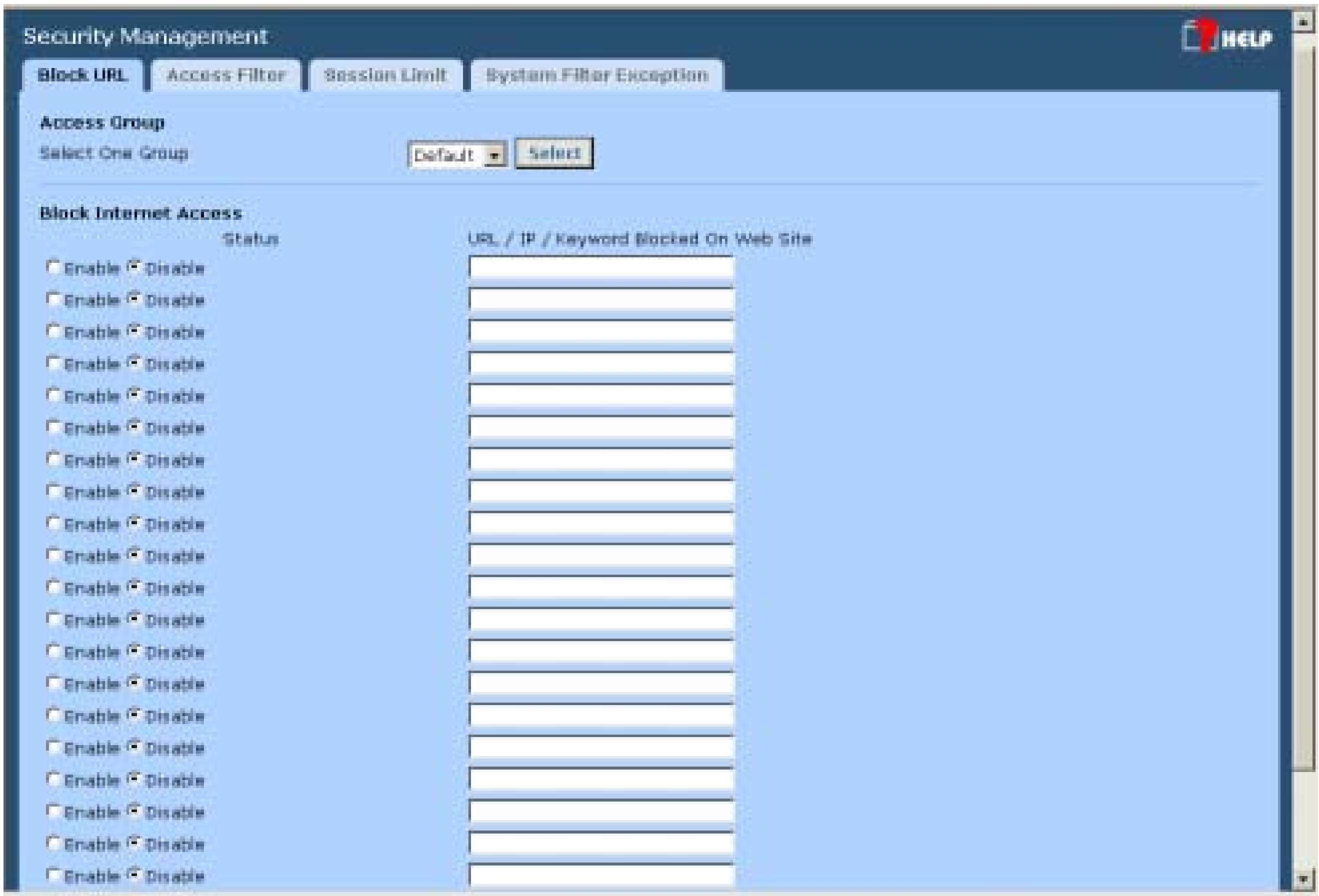


Figure 5-1: Block URL

Settings – Block URL

Access Group	This allows you have different blocking rules for different Groups of PCs. • All PCs (users) are in the *Default* Group unless moved to another group on the ***Host IP*** screen. • If you want the same restrictions to apply to everyone, select *Default* for the Group. In this case, there is no need to enter any Hosts on the ***Host IP*** screen. • If you wish to apply different restrictions on different Groups, select the desired Group, and click the "Select" button. The screen will update with data for the selected Group.
Block Internet Access	• **Enable/Disable** – Use this to Enable or Disable each setting, as required. • **Block URL/IP/Keyword** – Enter the URL, IP address or keyword you wish to block.

Access Filter

The network Administrator can use the Access Filter to gain fine control over the Internet access and applications available to LAN users.

- Five (5) user groups are available, and each group can have different access rights.
- All PCs (users) are in the *Default* group, unless assigned to another group on the ***Host IP*** screen.

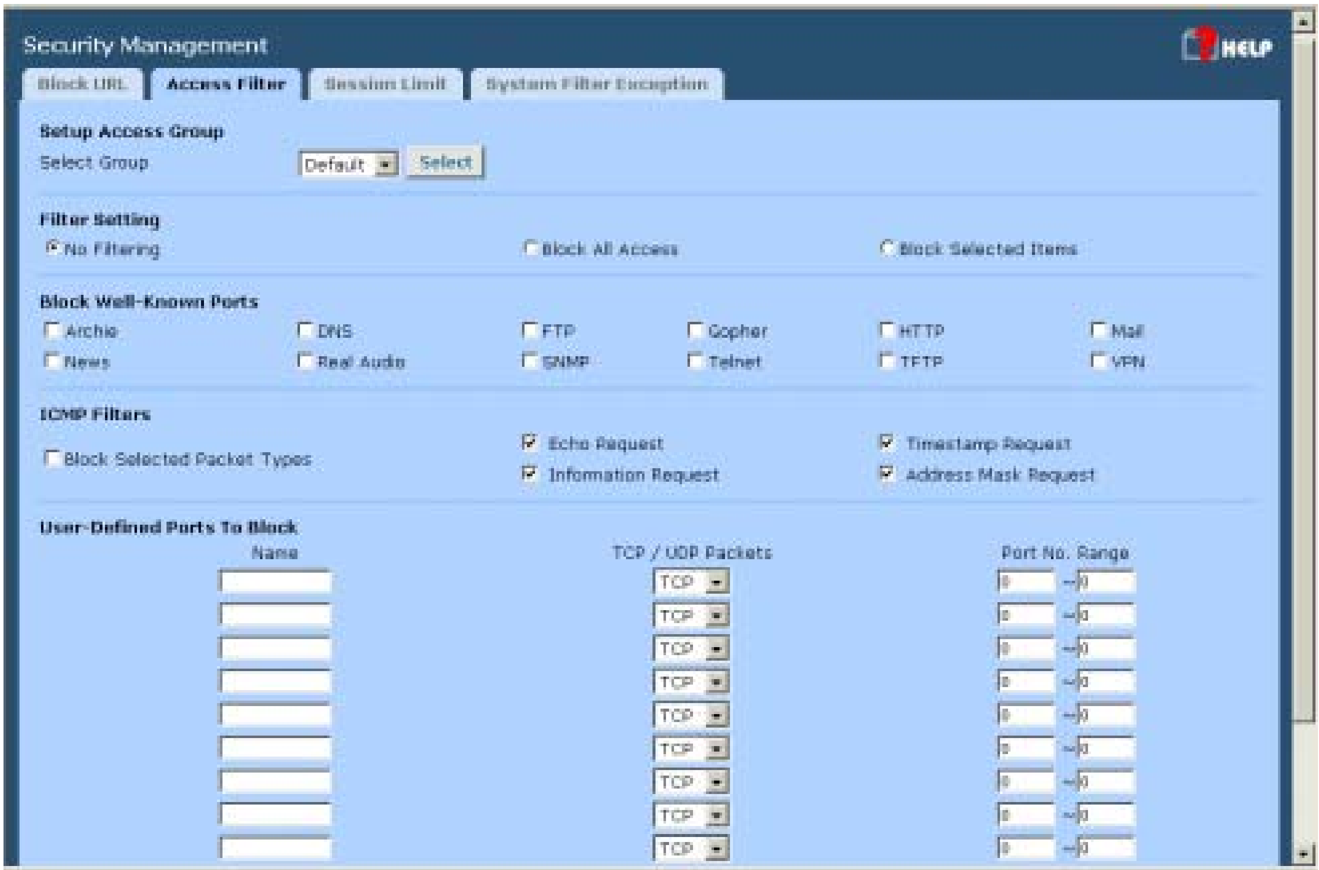


Figure 5-2: Access Filter

Settings – Block URL

Setup Access Group	**Select Group** - This allows you have different access rights for different Groups of PCs. • If you want the same restrictions to apply to everyone, select *Default* for the Group. In this case, there is no need to enter any Hosts on the ***Host IP*** screen. • If you wish to apply different restrictions on different Groups, select the desired Group, and click the "Select" button. The screen will update with data for the selected Group.

Filter Setting	Select the desired option for this Group: • **No filtering** – Nothing is blocked, Internet access is not restricted. • **Block All Access** – Everything is blocked, Internet access is not available. • **Block selected items** – Items selected on this screen are blocked. You can block well known services by using the checkboxes, or define your own filters.
Block Well-known ports	Select the services you wish to block. The current group will not be able to use any services which are checked.
ICMP Filters	IF you enable ICMP Filters function that mean it will block ICMP packets from local host send to remote site.
User-defined Ports to Block	This section is optional. It allows you to define your own filters if required. For each filter, the following information is required. • **Name** – Enter a meaningful name for this filter. • **TPC/UDP Packets** – Select either TCP or UDP, depending on which protocol is used by the service you wish to block. • **Port No. Range** – Enter the range of port numbers used by the service you wish to block. If only a single port is required, enter it in both fields.

Session Limit

This new feature allows to drop the new sessions from both WAN and LAN side. If the new sessions number are exceed the maximum sessions in a sampling time.

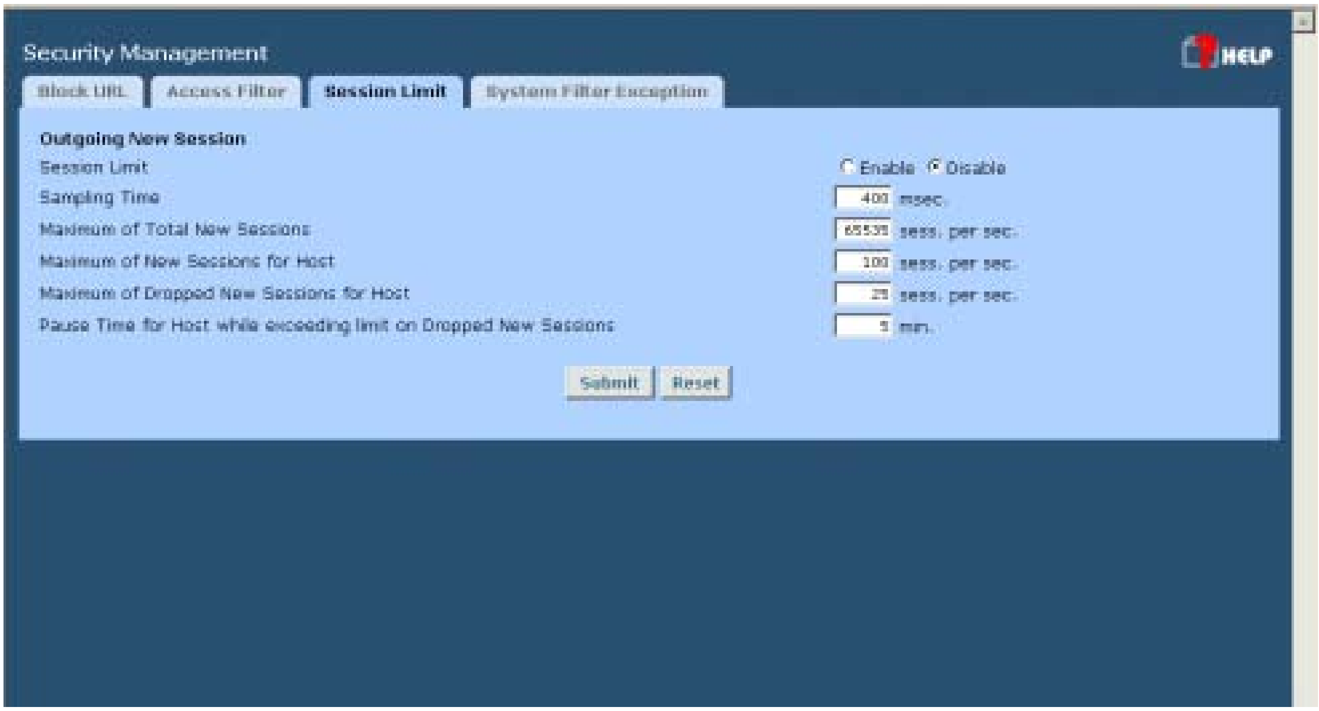


Figure 5-3: Session Limit

Session Limit

Outgoing New session	
Session Limit	Enable or disable “Session Limit” function. The default is Disable.
Sampling Time	The period to count the new session. Only those new sessions occurred in the most recently sampling time were be count for limit checking.(Default is 400 mil-sec)
Maximum of Total New session	If the number of new sessions for system exceed the maximum in the Sampling Time. Any new sessions in the system will be dropped. (Default: 65535 session/sec)
Maximum of New Sessions for Host	If the number of new sessions for the host exceeds the maximum in the sampling time. Any new session of the host will be dropped. (Default: session/sec)
Maximum of Dropped New Sessions for Host	If the number of dropped new sessions for the host exceeds the Maximum in the sampling time, any new session of the host will be dropped for the pause time.
Pause Time	Within the pause time, no new session of the suspended host could be served by system.(Default is 5 minutes)

System Filter Exception

System Firewall Exception Rules: The rules with which any received packets is complied, the packets will not processed by Firewall or NAT module, but to be processed directly by system protocol stack.

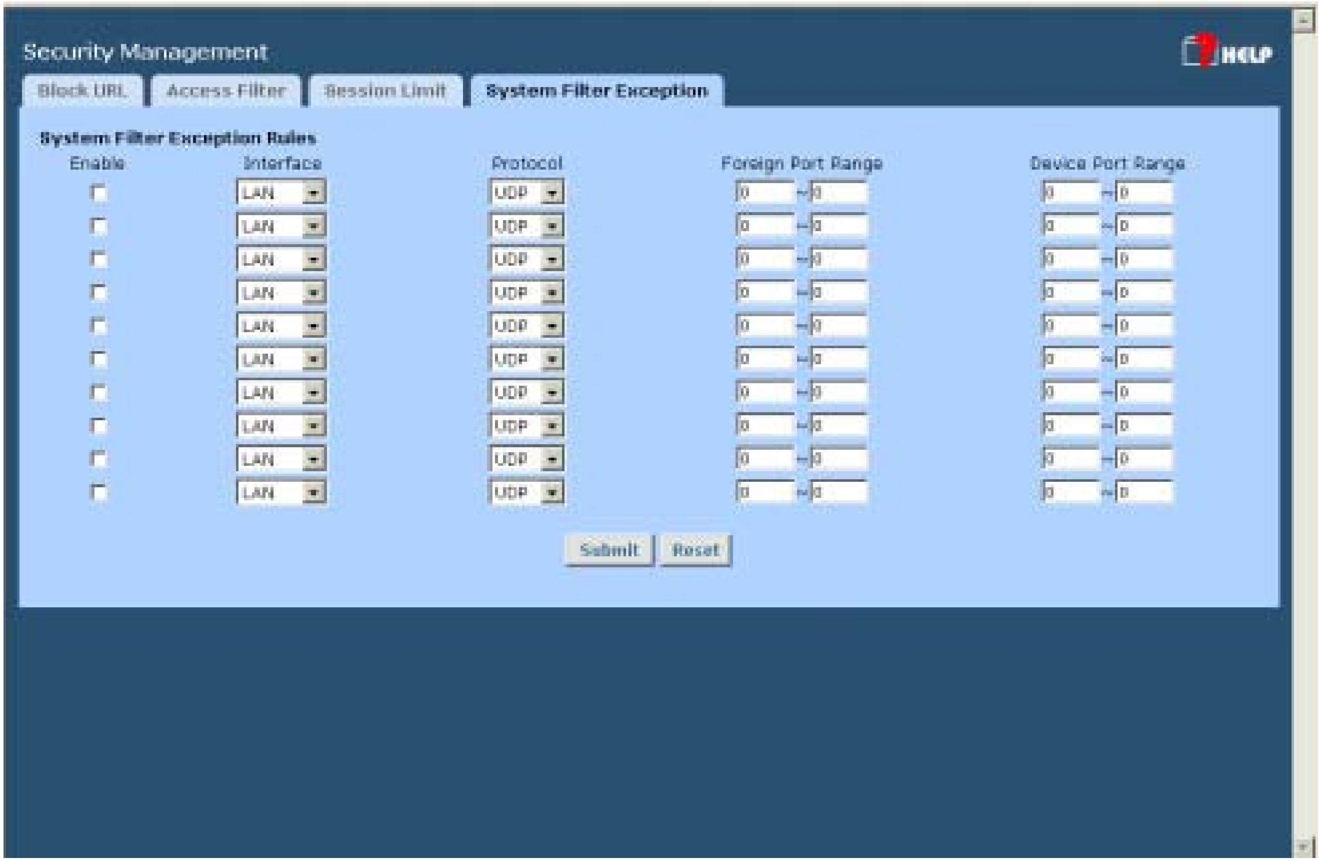


Figure 5-4: System Filter Exception

Setting - System Filter Exception

System Filter Exception Rules	**Enable** - The check box can allow you enable or disable firewall exception. **Interface** - You can select LAN, WAN1, WAN2 or ALL interfaces to be process by the system protocol stack. If you enable check box. **Protocol** - There are six protocols (UDP/TCP/ICMP/GRE/ESP/AH) to choose to let the packets directly process by the system protocol stack. **Foreign Port Range** - Select foreign port number range directly process by system protocol stack. If enable check box. **Device Port Range** - Select device port number range directly process by system protocol stack. If enable check box.

6: VPN Configuration

Overview

Virtual Private Network (VPN), is a connection between two end points. It allows private data to be sent securely over a public network, such as Internet. VPN establishes a private network that can send data securely between two networks. We call this is by creating a “tunnel”. A VPN tunnel connects the two PCs or networks

Planning the VPN

When planning your VPN, you must make following choices first.

1. If the remote end were a network, the two-endpoint network must have different LAN IP address ranges. If the remote endpoint is a single PC running a VPN client, its destination address must be a single IP address, with subnet mask of 255.255.255.255
2. Will you be using the Internet Key Exchange (IKE) setup, or Manual Keying, in which you must specify each phase of the connection.
3. What encryption level you are going to use (DES or 3DES)?

Note: The VPN 800/2 Firewall Router uses industry standard VPN protocol. However, due to variations in how manufactures interpret these standard, many VPN products are not interoperable. Although the VPN 800/2 Firewall Router can interoperate with many other VPN products. It is not possible for VPN 800/2 Firewall Router to provide specific technical support for every other product.

IPSec Global Setting

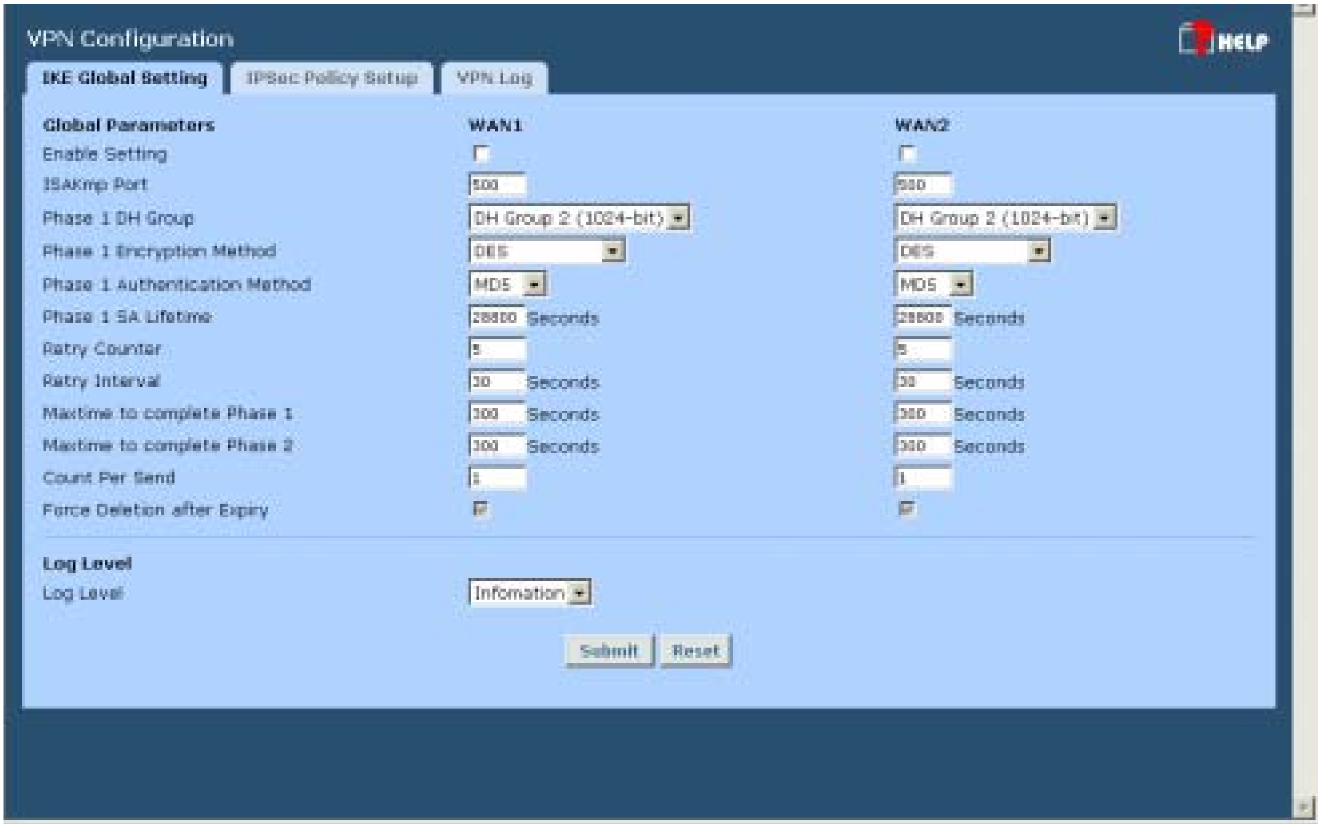


Figure 6-1: IPSec Global Setting

IP Global Setting

Global Parameters	**Enable** –If you enable check box either WAN1,WAN2 or both, this will start VPN global setting **ISAkmp Port**– Internet Security Association and Key Protocol Management (ISAkmp) is designed to negotiate, establish, modify and delete security associations and their attributes. In particular, it was assigned UDP port 500 by the IANA. **Phase 1 DH Group** – Use DH Group 1(768-bits),DH Group 2(1024-bits), Group 5 (1536-bits) to generate IPSec SA keys. **Phase 1 Encryption Method**– There are three data encryption methods available,DES, 3DES,and AES. **Phase 1 Authentication Method**– There are two authentication available. MD5 and SHA1 (Secure Hash Algorithm) **Phase 1 SA Life Time**– By default the Security Association lifetime is 28800 Sec. **Maxtime to complete phase 1** – The aim of phase 1 is to authenticate and establish a secure tunnel, which will protect further IKE negotiation. The maximum time default is 30 sec. **Maxtime to complete phase 2** – Really establish the IPSec SAs. By default the maximum time is 30 sec. **Count Per Send** – Number of duplicated packets for resend. **Force Deletion after Expiry** – Once SA get expired, tunnel will be removed and related resources will be released to the system.
Log Level	It is a VPN Log Level. Select a VPN log level that you like to display on VPN log.

Policy Setup

Policy Setup

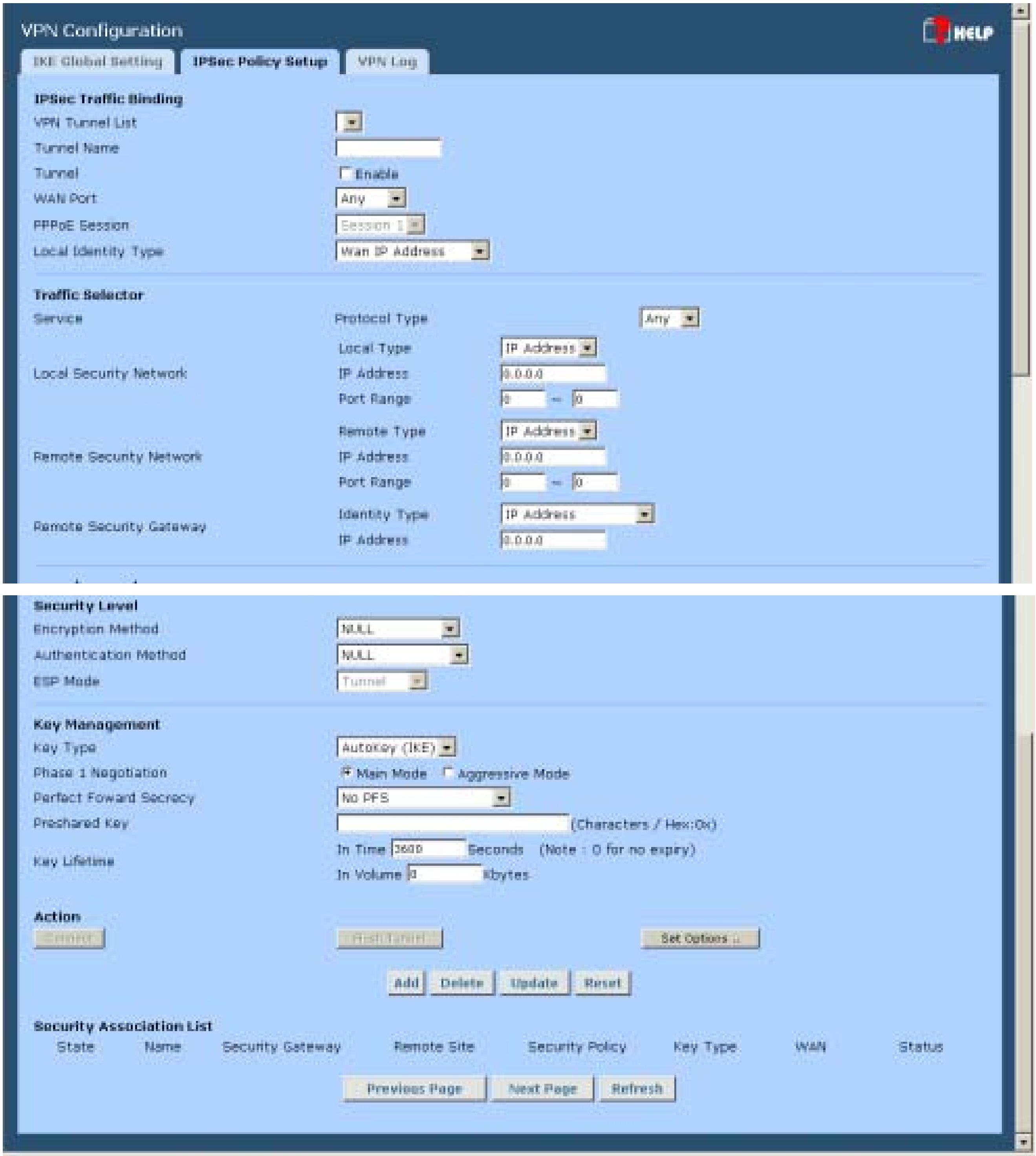


Figure 6-2: Policy Setup

VPN Policy Setup

IPSec Traffic Binding	**VPN Tunnel List**– It shows the tunnels that you have entered. The router can setup up to 20 tunnels **Tunnel Name**– In order to distinguish the tunnel, you have to give "Tunnel" a name.. **Tunnel** – Only enable tunnel check box, the tunnel can be connected. **WAN port** – You can choose WAN1, WAN2 or Any to make the VPN connection. **PPPoE Session**– If you are using PPPoE to make the connection, and some ISP offers multiple PPPoE session, you can select these PPPoE session to construct VPN tunnels. **Local Identity Type** – You can either choose your Local WAN IP or Domain name, Distinguished Name as your local identity.
Traffic Selector	**Service**– **Protocol Type:** You can choose either TCP/UDP/ICMP/GRE protocol as your connection protocol. By default the protocol type is "Any". **Local Security Network**– These entries identify the private network on this VPN router, the hosts of which can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN LAN-to-LAN connection. **Remote Security Network**– These entries identify the private network on the remote peer VPN router whose hosts can use the LAN-to-LAN connection. You can choose a single IP address, the subnet, or a selected IP range to make VPN connection **Remote Security Gateway –** You can either select remote side domain name or remote side IP address (WAN IP address) as your remote side security gateway.
Security Level	**Encryption Method** – It specifies the encryption mechanism to use. Data encryption makes the data unreadable if intercepted. There are three encryption method available; DES/3DES and AES. The default is null. **Authentication** – It specifies the packets authentication mechanism to use. Packets authentication proves that data comes from source you think it comes from. There are three authentications available. MD5, SHA1 and SHA2.

Key Management	**Key** – **Key Type:** there are two key types (manual key and auto key) available for the key exchange management. **Manual Key:** If manual key is selected, no key negotiation is needed. **AutoKey (IKE)-** There are two types of operation modes can be used. **Main mode** accomplishes a phase one IKE exchange by establishing a secure channel. **Aggressive Mode** is another way of accomplishing a phase one exchange. It is faster and simpler than main mode, but does not provide identity protection for the negotiating nodes. **Perfect Forward Secrecy** (PFS) – If PFS is enable, IKE phase 2 negotiation will generate a new key material for IP traffic encryption & authentication. Preshared Key – This field is to authenticate the remote IKE peer. **Key Lifetime**- This is specified the lifetime of the IKE generated Key. If the time expires or data is passed over this volumn, a new key will be renegotiated, By default, 0 is for no limit.

IPSec Policy options

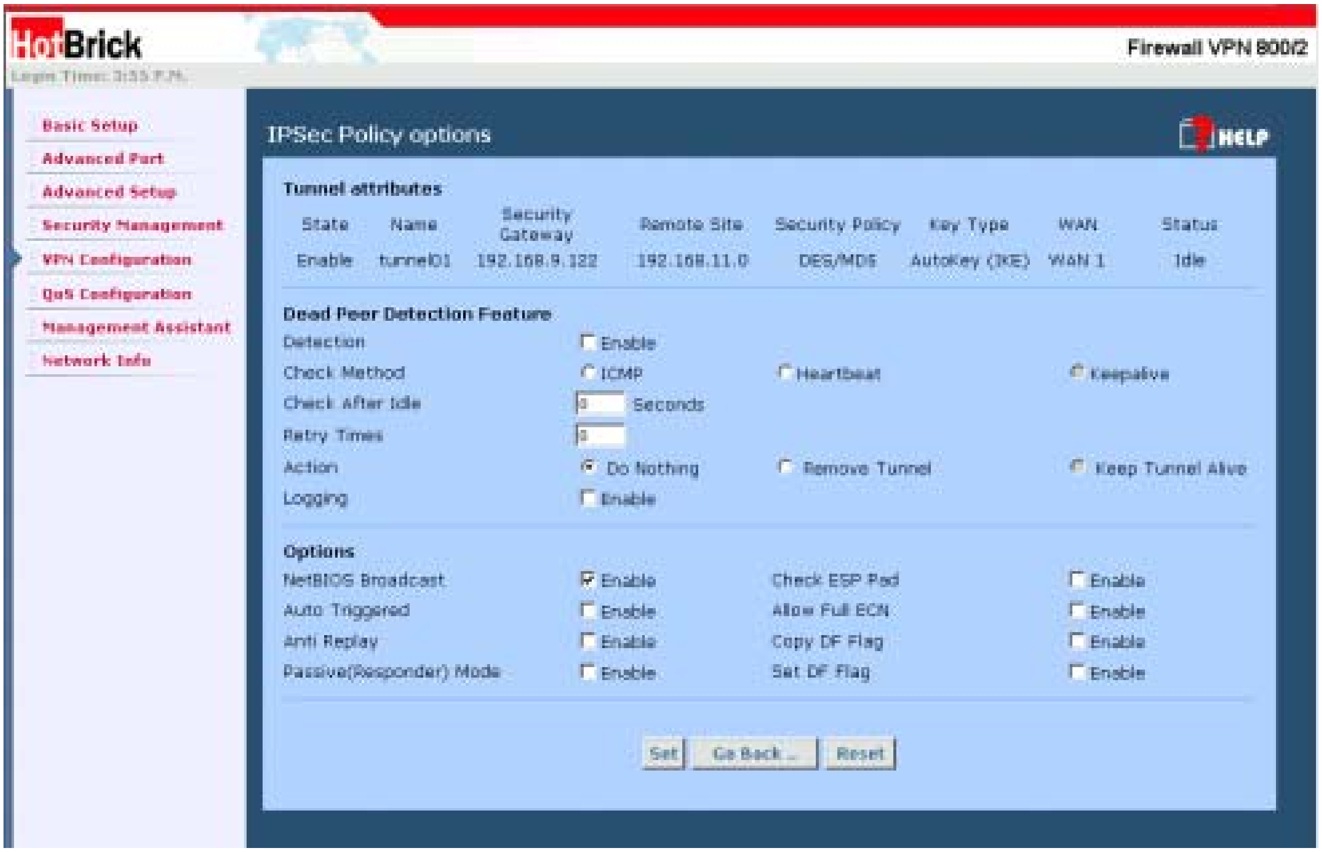


Figure 6-3: IPSec Policy Options

Tunnel Attribute	The current tunnel attribute that you just setup
Dead Peer Detection	If you like to utilize one of the wan port as a backup or plan failover function, you can enable Dead Peer Detection function. **Check Method** – You can either choose ICMP, Heartbeat, detecting the remote site VPN tunnel if it is alive or not

Set Options	**NetBIOS Broadcast-** This is used to forward NetBIOS broadcast across the Internet. **Auto Trigger**–This is help to keep up the IPSec connection tunnel. It can be re-established immediately, if a connection is dropped and detected. **Anti Replay** – It ensures to keep track of IP packet-level security in order. **Passive mode** – This means that your PC establishes the data connection. If you enable passive mode. **Check ESP Pad** – If enable ESP(Encapsulating Security Payload),it will check ESP padding. **Allow Full ECN** – Enable will allow full Explicit Congestion Notification (ECN). ECN is a standard proposed by the IETF that will cut down on network congestion and routers dropping packets. **Copy DF Flag** – When an IP packet is encapsulated as payload inside another IP packet, some of the outer header fields can be newly written, and others are determined by the inner header. Among these fields is the IP DF (don't fragment) flag. When the inner packet DF flag is clear, the outer packet may copy it or set it; however, when the inner DF flag is set, the outer header MUST copy it. **Set DF Flag-** If this DF (Do not Fragment) flag is set, it means the fragmentation of this packet at the IP level is not permitted.

7: QoS Configuration

Overview

The VPN 800/2 Firewall Router provides QoS, which supports the high quality of network service. Because it will classify outgoing packets based on some policies defined by users, make some real-time applications to get better response or performance.

QoS Setup

The following web page management are guiding you how to setup QoS and make QoS work.

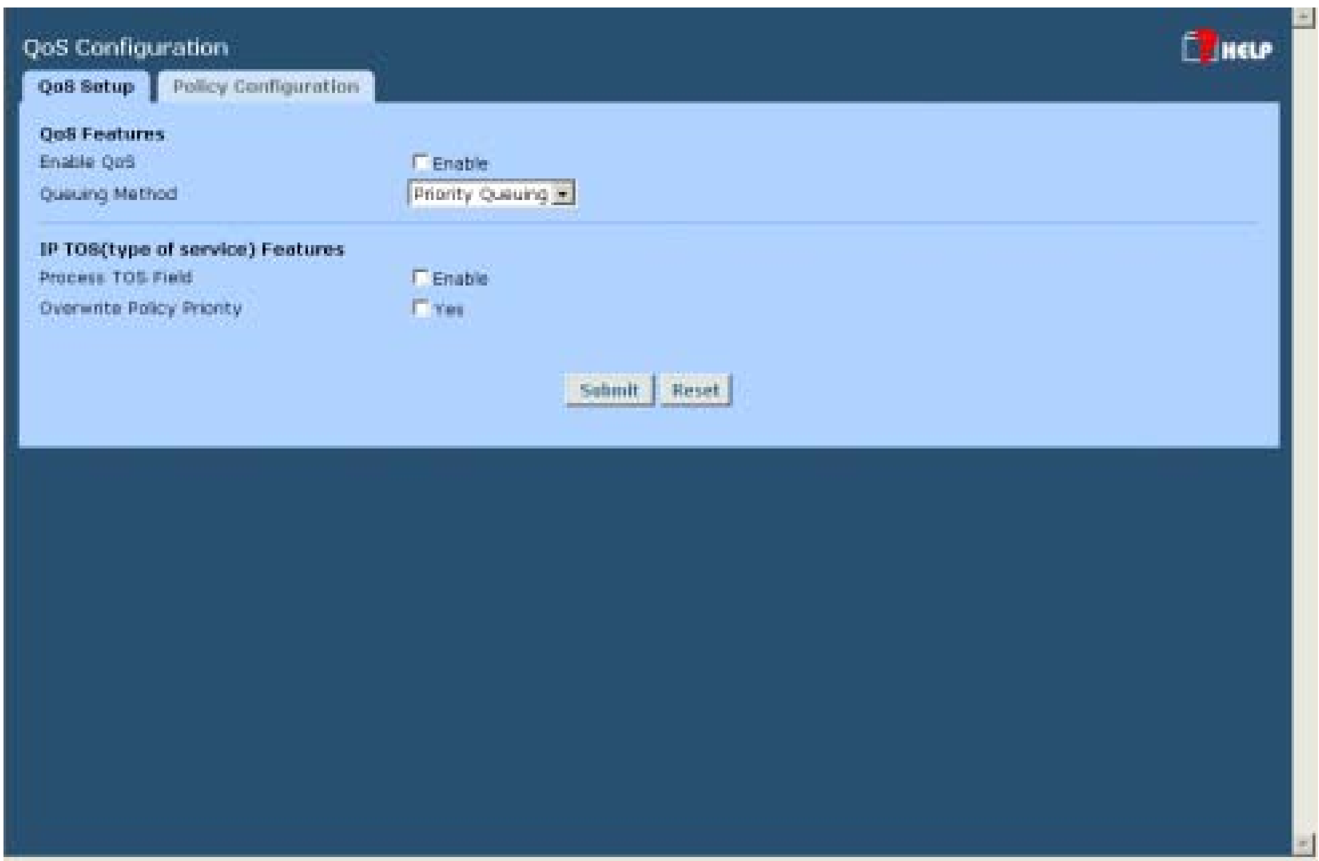


Figure 7-1: QoS Setup

Data – QoS Setup.

QoS Feature	◆ **Enable QoS** – This will allow users enable QoS function. • **Queuing Method** – The methods that how you manage your queue." Priority queuing". It is one of the first queuing variations to be wildly implemented.
IP TOS (Type of Service) Feature	• **Process TOS Field** –An 8 bits field in the IP packet header designed to contain values indicating how each packet should be handled in the network. If you choose "enable" then it will enable this function to process IP Type of Service field. • **Overwrite policy priority** – Choose "yes" to set the priority of TOS field in IP packet overwrite the priority defined in policy configuration

Policy Configuration

When you use QoS, you must define some policies to make some packets to have higher priority to pass through.

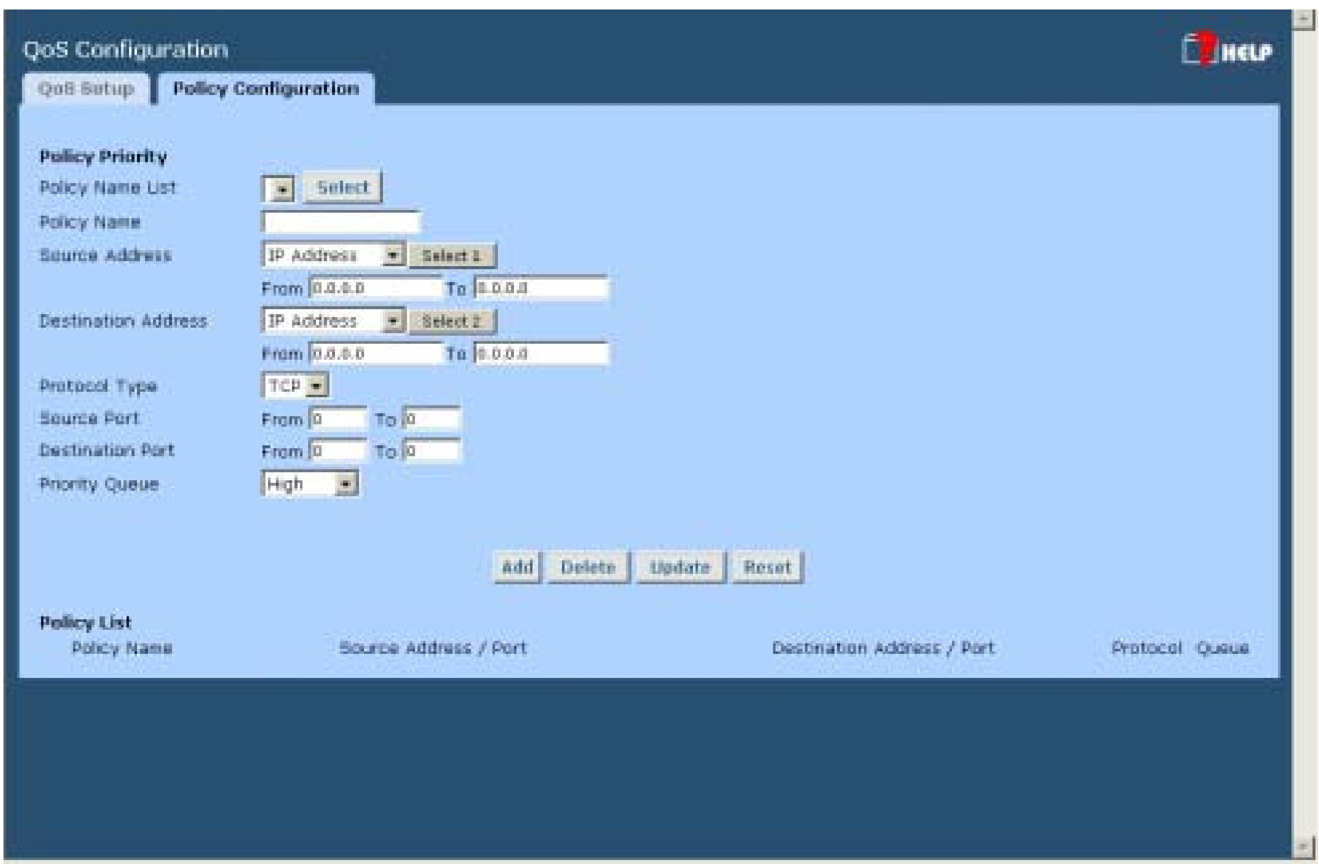


Figure 7-2: Policy Configuration

Data – Policy Configuration.

Policy Priority	This section identifies each policy • **Policy Name List** – When adding a new Policy, ignore this list. To edit an existing entry, select it from the list, and click the "Select" button. The data fields will then be updated with data for the selected entry. • **Policy Name** – Enter a suitable name. Generally, you should use the "Policy Name" for the network traffic. • **Source Address** – Define the source address of packets here. It has two types like IP address or MAC address. If you select IP address, you can define IP address range; otherwise define up to four MAC addresses. • **Destination Address** – Define the destination address of packets here. The explanation is as the same as above. • **Protocol Type** – The field defines traffic packet type, i.e. IP,TCP and UDP. • **Source Port** – Define the source port of packets here. • **Destination Port** – Define the destination port of packets here. • **Priority Queue** – It defines a packet if it meets all conditions defined above, it will be serviced with some priority level.

8: Management Assistant

Overview

The following advanced features are provided.

- SNMP
- Email Alert
- SNMP
- Syslog
- Upgrade Firmware

This chapter contains details of the configuration and use of each of these features.

SNMP

This section is only useful if you have SNMP (Simple Network Management Protocol) software on your PC. If you have SNMP software, you can use a standard MIB II file with the VPN 800/2 Firewall Router.

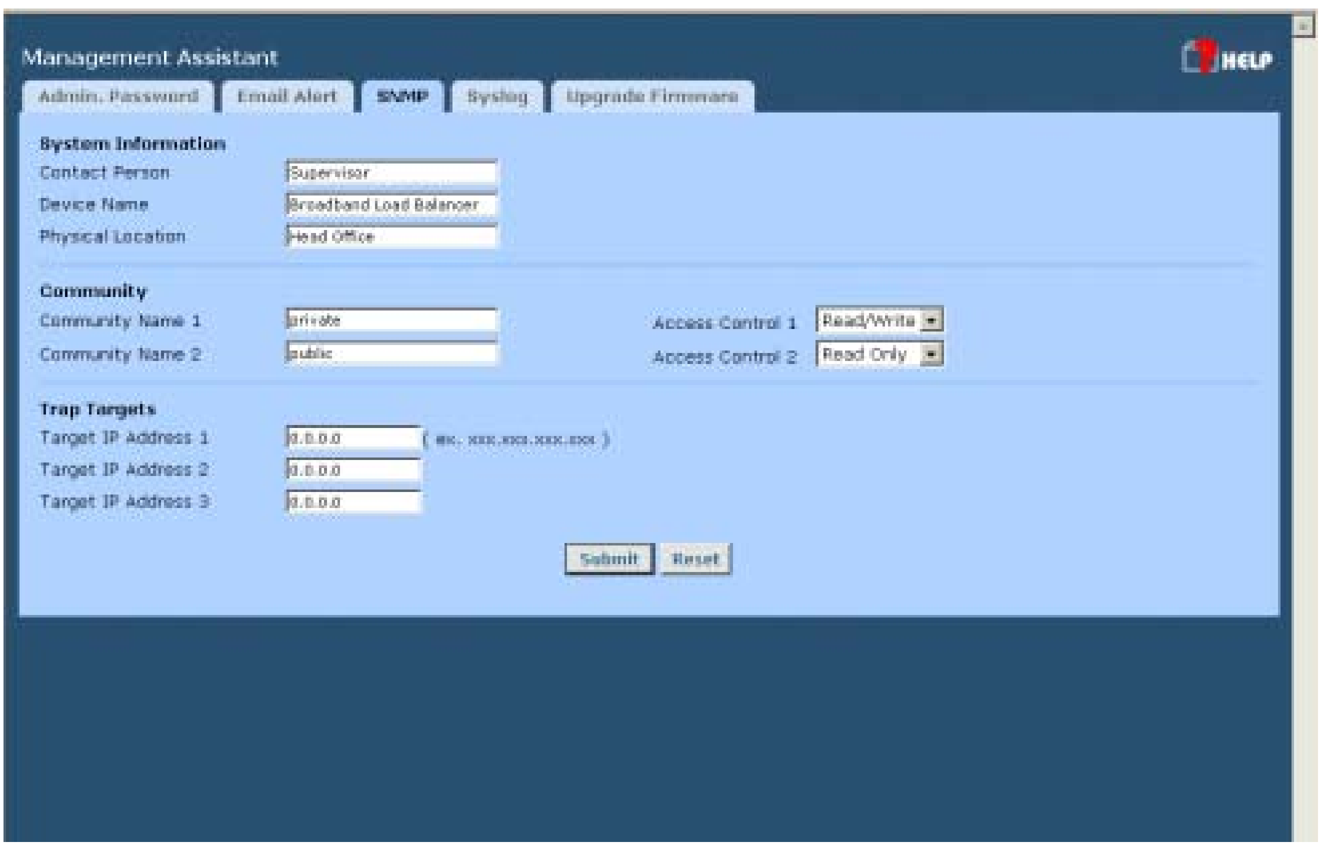


Figure 8-1: SNMP

Settings – SNMP

System Information	• **Contact Person** – The name of the person responsible for this device. • **Device name** – The name of VPN 800/2 Firewall Router. • **Physical Location** – The location of the VPN 800/2 Firewall Router.
Community	It is a relationship between a SNMP agent and a set of SNMP manager that defines authentication, access control, and proxy characteristics.
Trap Targets	Enter the IP address of any targets (PCs running SNMP software) to which you want traps to be sent. All traps are level 1.

Email Alert

This feature will send a warning Email, inform system administrator that one of the WAN ports was disconnected.

Email Alert – You can choose to enable or disable it to send a warning email.

Email Sender Address – It is an email address which will send the warning email.

Email (SMTP) Server Address – It is an email server address the warning email will be sent to.

Email Recipient Address – It is an email address of system administrator the email will be sent to.

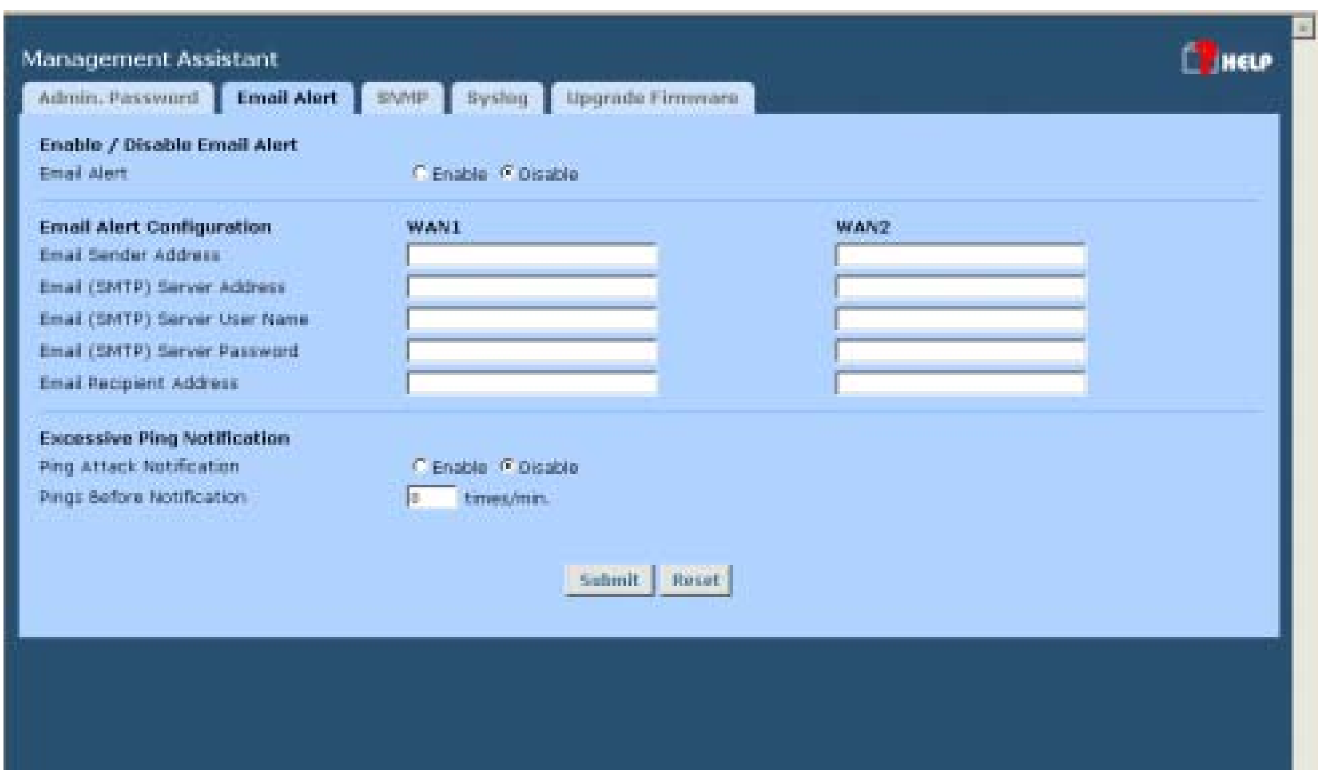


Figure 8-2: Email Alert

Settings – Email Alert

Enable/Disable Email Alert	• **Enable** – This will enable email alert to send a warning email when WAN port was disconnected. • **Disable** – This will disable email alert not to send a warning email when WAN port was disconnected.
Email Alert Configuration	**Email Sender Address**- It is an email address that sends a warning email to a recipient. Inform that a recipient checks if there is any problem on WAN ports or not. **Email (SMTP) Server Address -** It is an email sever a warning email will be sent to. If you are enabled email alert. For example: mail.domain.com. **Email(SMTP) server user name –** This is the user name of email sender for authentication (optional). **Email(SMTP)server password -** This is the user password **Email (SMTP) Server Address** - is an email sever a warning email will be sent to. If you are enabled email alert. For example: mail.domain.com **Email Recipient Address** - It is an email address a warning email will be sent to. Usually it is system administrator email address. For example: admin@mail.domain.com
Excessive Ping Notification	This feature is useful to prevent ICMP attack from WAN or LAN. It will drop the packets if the ping times are excessive the threshold value. It will send email to the administrator, if email is enabled.

Syslog

This feature can send real time system information on the web page or to the specified PC.

Syslog Configuration – Syslog Configuration allow you where to send system information to other machine or not. There are up to three machines you can choose to send your system log.

Message Status– Messages send only keep when "keep send message" checked. Currently we keep last 100 messages in the RAM area, they will clear when reboot or power off.

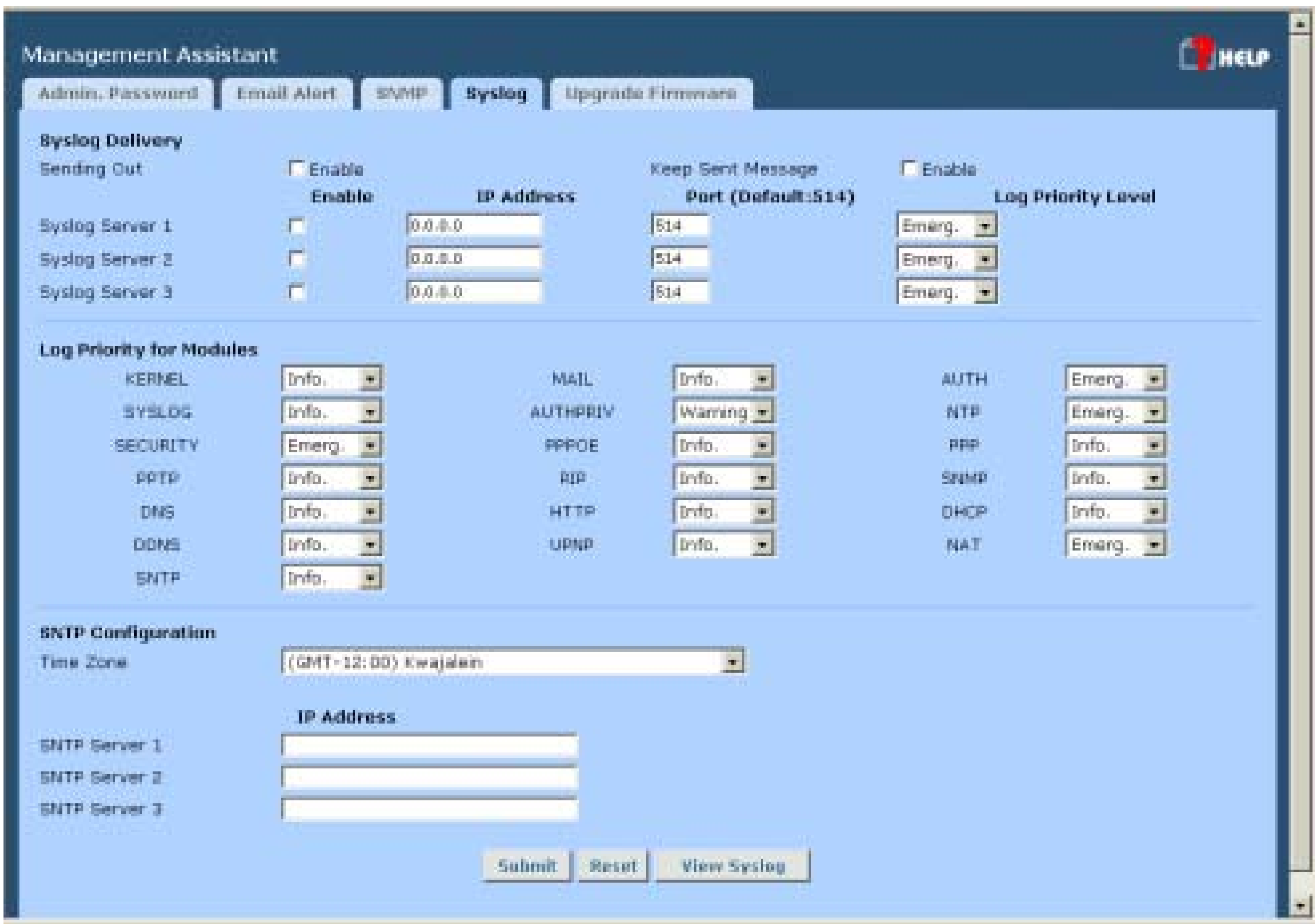


Figure 8-3: Syslog

Syslog Configuration

Syslog Delivery	**Sending out –** Check this, if you want to send syslog messages to other machine. **Keep Send messages** – Check this, if you want to keep sent messages, otherwise the sent message will be delete. **Syslog Server - IP address:** Up to 3 syslog servers can be used.**Enable:** You can enable or disable each server temporarily. **Port:** If your syslog server does not use the default port, you can change it.
Log Priority For Modules	The syslog messages are divided into 8 levels, from Emergency to Debug level. The lower level, the less messages will be generated. Emergency is the lowest priority level, and Debug is the highest one.
SNTP Configuration	**Time Zone** – You can setup system up time using SNTP (**S**imple **N**etwork **T**ime **P**rotocol), and there are 3 SNTP server that you can define on the SNTP configuration.

Admin Password

The password screen allows you to assign a password to the Firewall Router.



Figure 8-4: Admin Password Screen

Enter the desired password, re-enter it in the *Verify Password* field, then save it.

When you connect to the Load Balancer with your Browser, you will be prompted for the password when you connect, as shown below.



Figure 8-5: Password Dialog

- Enter "Admin" for the *User Name*.
- Enter the password for the VPN 800/2 Firewall Router, as set on the *Admin Password* screen above.

Upgrade Firmware

This Upgrade Firmware Screen allows you to upgrade firmware or backup system configuration by using HTTP upgrade.

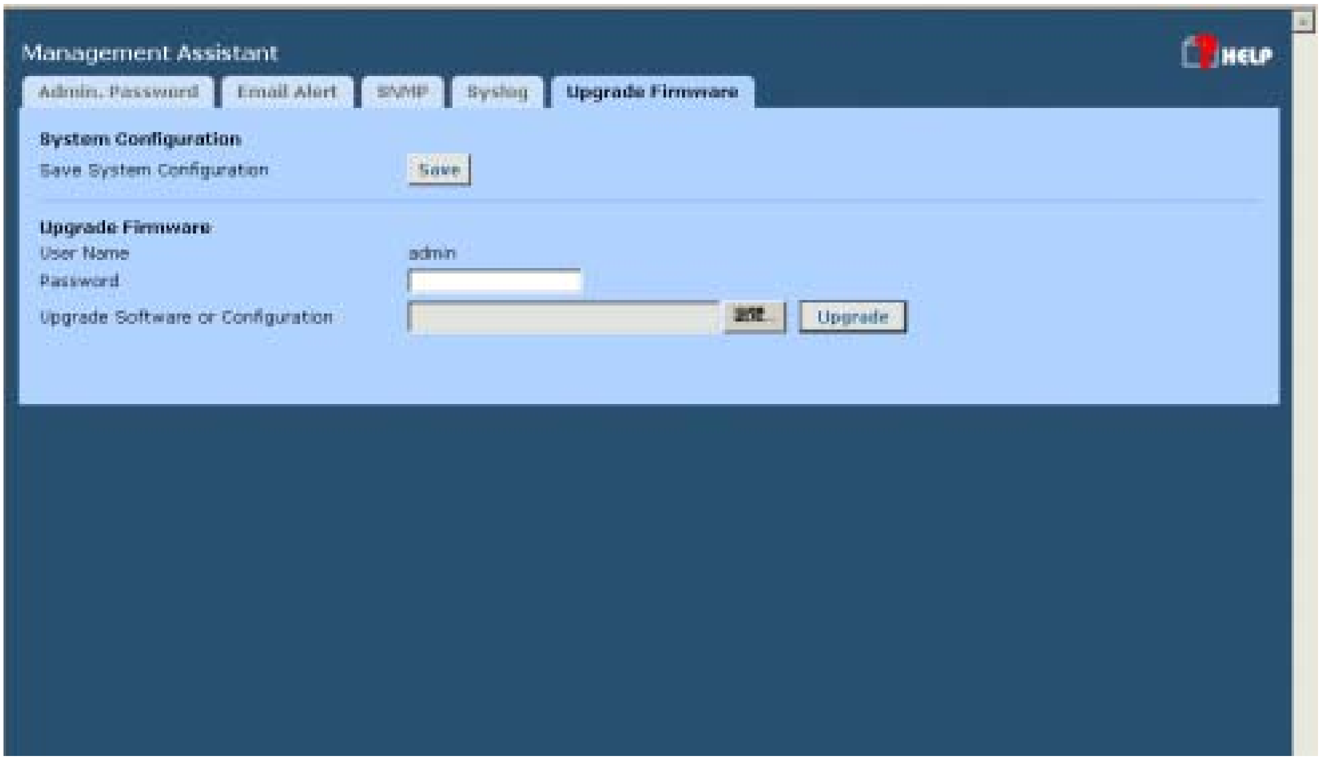


Figure 8-6: Upgrade Firmware

- You can backup your system configuration by press “save” button of Save System Configuration. It will save the system configuration for you. (Notice: You have to refresh the browser after you saved the system configuration file)
- You also can do firmware upgrade by input the correct password and the file name of your firmware. Remember do not Reset or Restart the device while update new firmware, because it may cause system to crash.

9: Advanced LAN Configuration

Overview

These screens and settings are provided to deal with non-standard situations, or to provide additional options for advanced users.

Existing DHCP Server

If your LAN already has a DHCP Server, and you wish to continue using it, the following configuration is required.

- The DHCP Server function in the Load Balancer must be **disabled**. This setting is on the ***LAN & DHCP*** screen.
- Your DHCP Server must be configured to provide the VPN 800/2 Firewall Router's LAN IP address as the "Default Gateway".
- Your DHCP Server must provide correct DNS addresses to the PCs.

Routing

This section is only relevant if your LAN has other Routers or Gateways.

- If you don't have other Routers or Gateways on your LAN, you can ignore the ***Routing*** page completely.
- If your LAN has other Gateways and Routers, you must configure the Static Routing screen as described below. You also need to configure the other Routers.

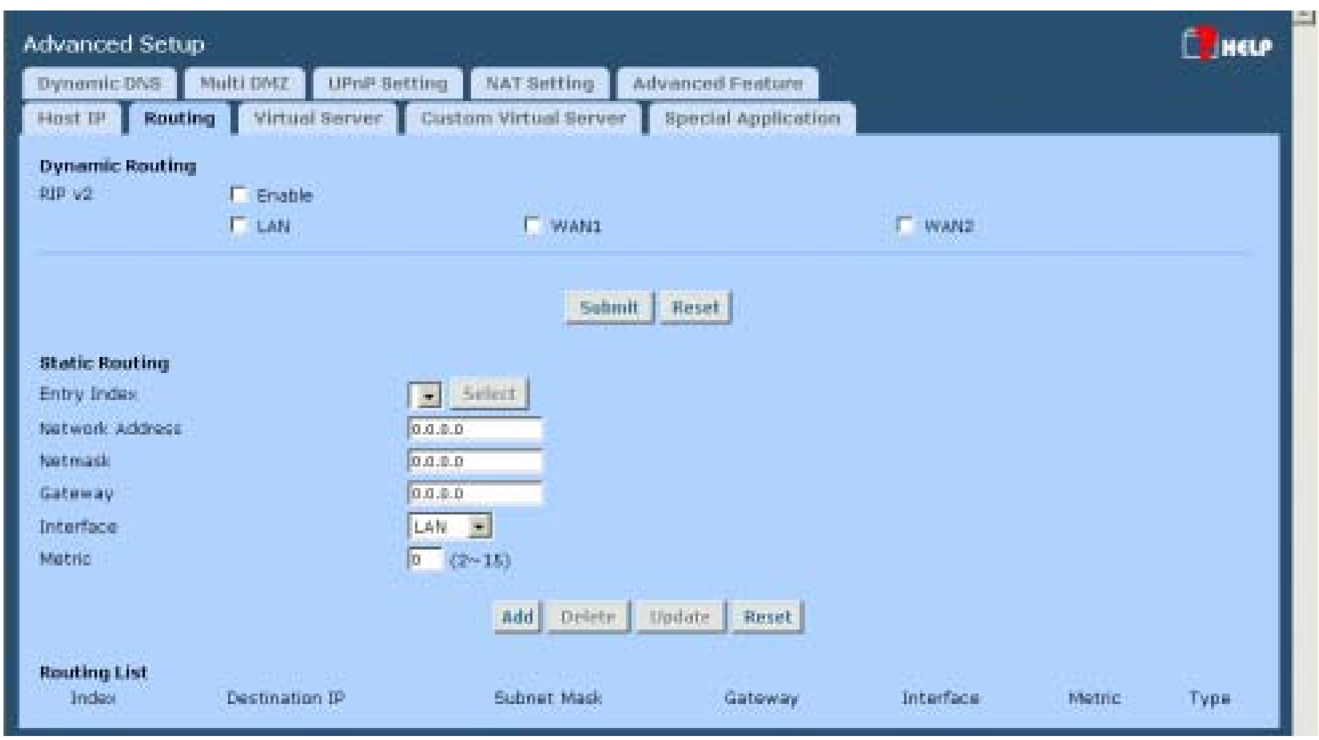


Figure 9-1: Routing

Note:

If there is an entry or entries in the Routing table with an Index of zero (0), these are System entries. You cannot modify or delete these entries.

Settings – Routing

Dynamic Routing	• **RIP v2** – This acts as “master” switch. If enabled, the selected WAN or LAN will run RIPv1/v2, otherwise they don’t have RIP function. • **LAN, WAN1, WAN2** – If enabled, any WAN or LAN can execute RIP function.
Static Routing	**Network Address** - The network address of the remote LAN segments. For standard class "C" LANs, the network address is the first 3 fields of the Destination IP Address. The 4th (last) field can be left at 0. **Netmask** -The Network Mask for the remote LAN segments. For class "C" networks, the default mask is 255.255.255.0 **Gateway** -The IP Address of the Gateway or Router which the VPN 800/2 Firewall Router must use to communicate with the destination above. (NOT the router attached to the remote segment.) **Interface** - Select the correct interface, usually "LAN". The "WAN" interface is only available if NAT (Network Address Translation) is disabled. **Metric** - The number of "hops" (routers) to pass through to reach the remote LAN segment. The shortest path will be used.

Configuring Other Routers on your LAN

All traffic for devices not on the local LAN must be forwarded to the Load Balancer, so that they can be forwarded to the Internet. This is done by configuring other Routers to use the VPN 800/2 Firewall Router as the *Default Route* or *Default Gateway*, as illustrated by the example below.

Static Routing - Example

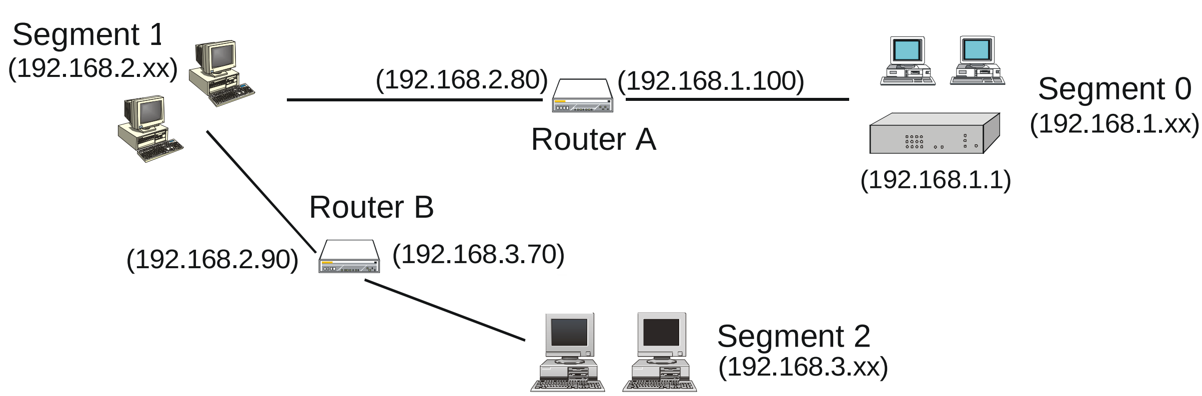


Figure 9-2: Routing Example

For the VPN 800/2 Firewall Router Gateway's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the VPN 800/2 Firewall Router requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	2
Entry 2 (Segment 2)	
Destination IP Address	192.168.3.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.1.100
Interface	LAN
Metric	3

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.1
Metric	2

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.2.80
Interface	LAN
Metric	3

10: Operation and Status

Operation

Once both the VPN 800/2 Firewall Router and the PCs are configured, operation is automatic. However, there are some situations where additional Internet configuration may be required: Refer to *Chapter 4 - Advanced Features* for further details.

System Status

Use the ***System Status*** link on the main menu to view this screen.



Figure 10-1: System Status

Data – System Status

WAN Information	• **Connection Status** – Current status – either "Connected" or "Not connected". • **Connection Type** – The type of connection used – DHCP, Fixed IP, PPPoE, or PPTP. • **"Force Renew"** button– Only available if using a dynamic IP address (DHCP). Clicking this button will perform a DHCP "Renew" transaction with the ISP's DHCP server. This will extend the period for which the current WAN IP address is allocated to you. • **IP Address** – The IP address of the VPN 800/2 Firewall Router, as seen from the Internet. This IP Address is allocated by the ISP (Internet Service Provider) • **Subnet Mask** – The Network Mask (Subnet Mask) for the IP Address above. • **Domain Name IP Address** – The address of the current DNS (Domain Name Server. • **MAC Address** – The MAC (physical) address of the VPN 800/2 Firewall Router, as seen from the Internet.
LAN Information	• **IP Address** – The LAN IP Address of the VPN 800/2 Firewall Router. • **Subnet Mask** – The Network Mask (Subnet Mask) for the IP Address above. • **MAC Address** – The MAC (physical) address of the VPN 800/2 Firewall Router, as seen from the local LAN. • **DHCP Server** – The status of the DHCP Server function - either "Enabled" or "Disabled".
Device Information	• **Firmware Version** – Version of the Firmware currently installed. • **NAT** – Status of the *NAT* feature – either “Enable” or “Disable”. • **Load Balance** – Status of the *Load Balance* feature – either “Enable” or “Disable”. • **Virtual Server** – Status of the *Virtual Server* feature – either "Enabled" or "Disabled". • **Special Applications** – Status of the *Special Applications* feature – either "Enabled" or "Disabled". • **DMZ** – Status of the *DMZ* feature – either "Enabled" or "Disabled". • **Block URL** – Status of the *Block URL* feature – either “Enable” or “Disable”. • **Hardware ID** – The manufacturers ID for this particular device.
Device Statistics	• **System UpTime** – The time since the system of a device was last reinitialized. • **CPU Usage** – The current usage percentage of CPU. • **Memory Usage** – The current usage percentage of Memory (Heap & Queue).

Buttons	• **Refresh** – Update the data on screen. • **Restart** – Restart (reboot) the VPN 800/2 Firewall Router. • **Restore Factory Defaults** – This will delete all existing settings, and restore the factory default settings. See below for details.

Restore Factory Defaults

When the "Restore Factory Defaults" button on the ***Status*** screen above is clicked, the following screen is displayed.

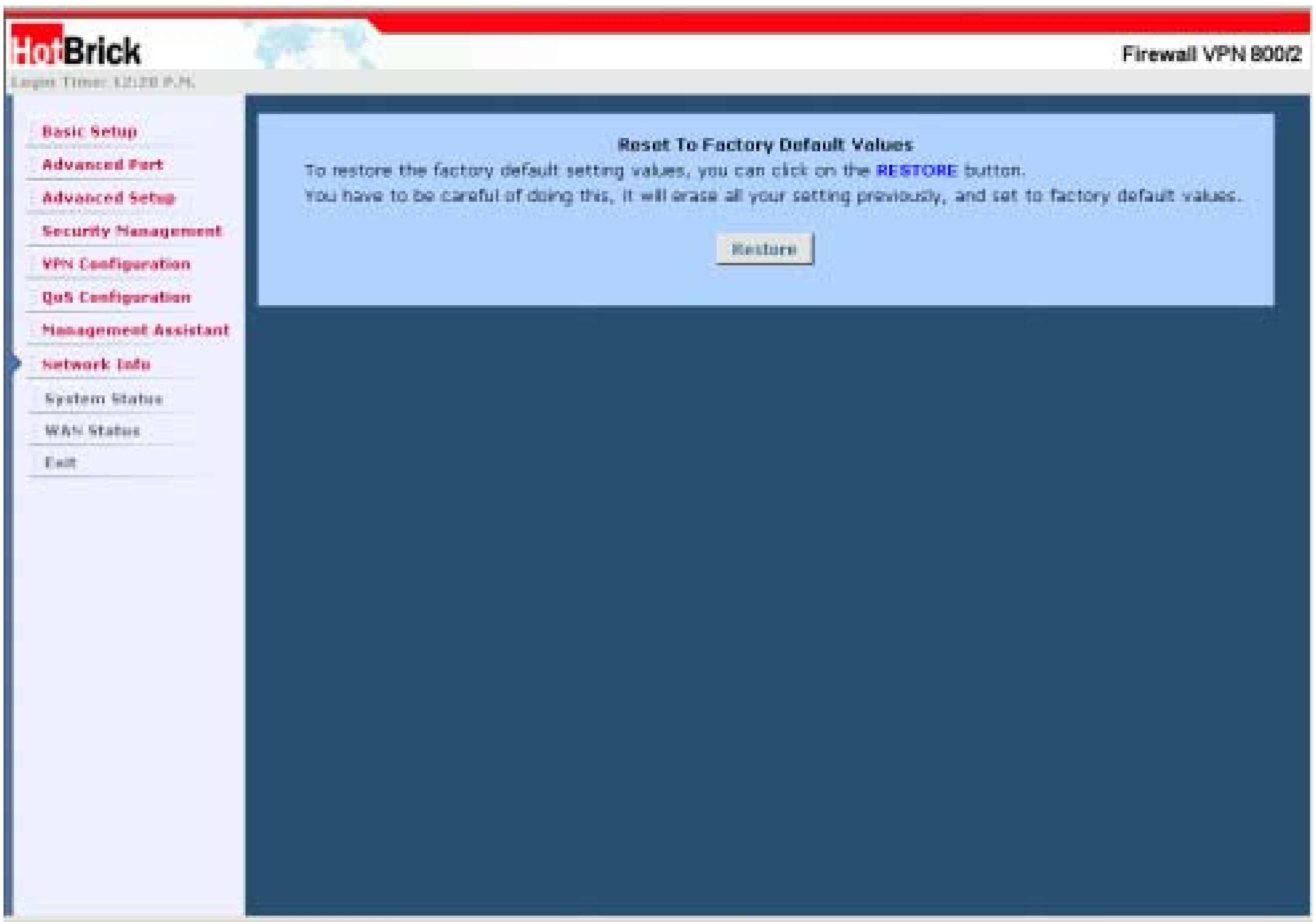


Figure 10-2: Restore Factory Defaults

If the "Restore Default Value" button on this screen is clicked:

- ALL of your settings will be erased.
- The default IP address, password and ALL other settings will be restored to the factory default values.
- The DCHP server function will be enabled.

These changes may mean that the current connection is invalid, and you will have to re-connect to the VPN 800/2 Firewall Router using its default IP address (192.168.1.1).

WAN Status

Use the ***WAN Status*** link on the main menu to view this screen.

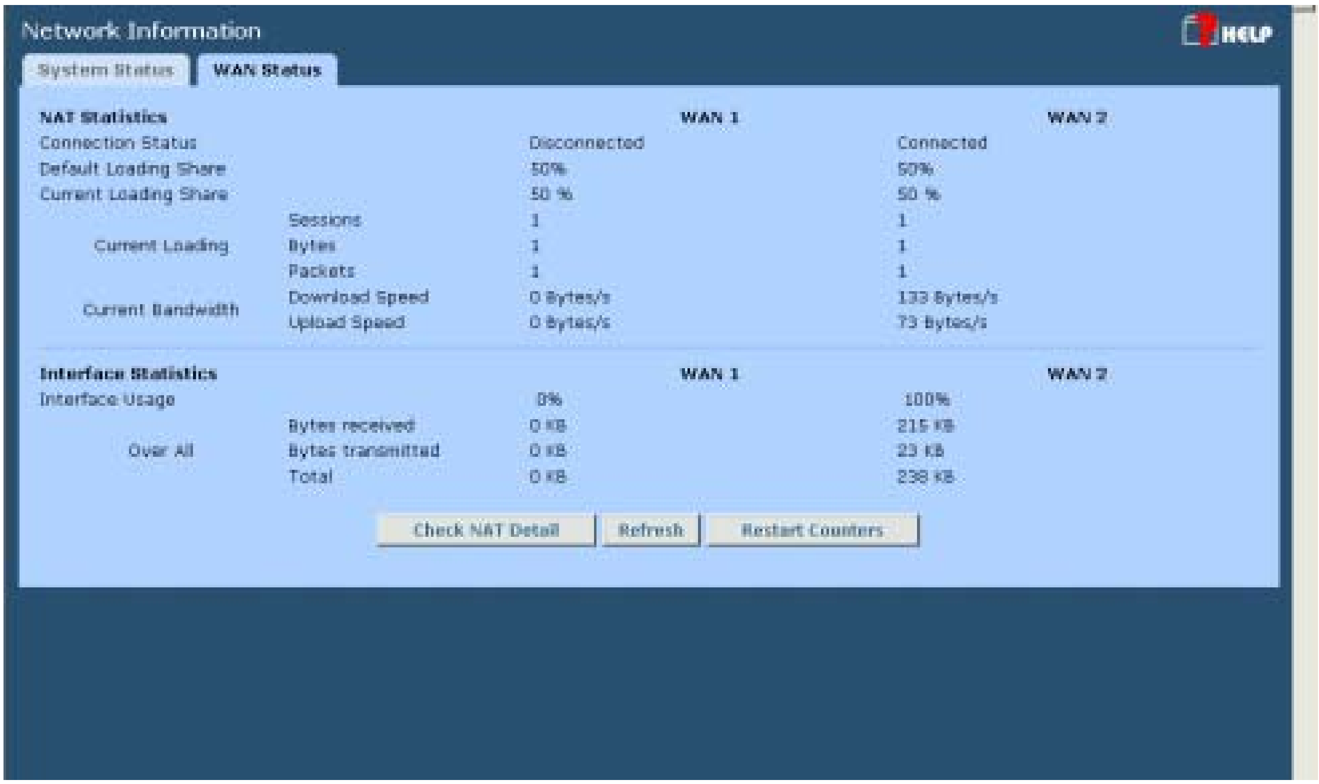


Figure 10-3: WAN Status

Data – System Status

NAT Statistics	This section displays data for each WAN port. • **Connection status** – This will display either *Connected* or *Not Connected*. • **Default Loading Share** - The default traffic loading between the WAN ports. • **Current Loading Share** – The current traffic loading between the WAN ports. • **Current Loading** – The number of sessions, Bytes and Packets currently being processed on each port. • **Current Bandwidth** – The current Download and Upload speeds on each WAN port. • "Check NAT Detail" will display the ***NAT Status*** screen, described below.
Interface Statistics	This section displays cumulative statistics. Use the "Restart Counter" button to restart these counters when required.

NAT Status

This screen is displayed when you click the "Check NAT Detail" button on the ***WAN Status*** screen.



Figure 10-4: NAT Status

Data – NAT Status

LAN IP Info	• **IP Address** – The LAN IP Address of the VPN 800/2 Firewall Router. • **Mask Address** – The Network Mask (Subnet Mask) for the IP Address above.
Active WAN IP Info	There is one (1) row for each active connection. For each connection, the following data is shown. • **IP Address** – The WAN (Internet) IP Address of the VPN 800/2 Firewall Router. • **Mask Address** – The Network Mask (Subnet Mask) for the IP Address above
NAT Timeouts	This displays the current timeout values for TCP and UDP connections.
TCP Prosperity	This displays the MSS (Maximum Segment Size) and Maximum Windows size for TCP packets.

NAT Traffic	This section displays statistics for both outgoing (LAN to Internet) and Incoming (Internet to Local) traffic.
NAT Connections	This displays the current number of active connections. For further details, click the "View Connection" list button.
Errors	Statistics are displayed for Checksum errors, number of retries, and number of bad packets.
Misc.	This displays the total IP packets and reserved address.

Appendix A
Specifications

Model	Hotbrick VPN 800/2 Firewall Router
Dimensions	120mm (W) x 427mm (D) x 43.4mm (H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	10 Ethernet: 8 * 10/100BaseT (RJ45) auto-Switching Hub ports for LAN devices 2 * 10/100BaseT (RJ45) for WAN
LEDs	8 LAN 2 WAN 2 Status 1 Power
Power Input	AC 115V-230V @ 0.5A

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Appendix B
Windows TCP/IP Setup

Overview

TCP/IP Settings

If using the default Load Balancer settings, and the default Windows 95/98/ME/2000 TCP/IP settings, no changes need to be made.

- By default, the VPN 800/2 Firewall Router will act as a DHCP Server, automatically providing a suitable IP Address (and related information) to each PC when the PC boots.
- For all non-Server versions of Windows, the default TCP/IP setting is to act as a DHCP client.
- If you wish to check your TCP/IP settings, the procedure is described in the following sections.
- If your LAN has a Router, the LAN Administrator must re-configure the Router itself.

Checking TCP/IP Settings - Windows 9x/ME:

1. Select *Control Panel - Network*. You should see a screen like the following:

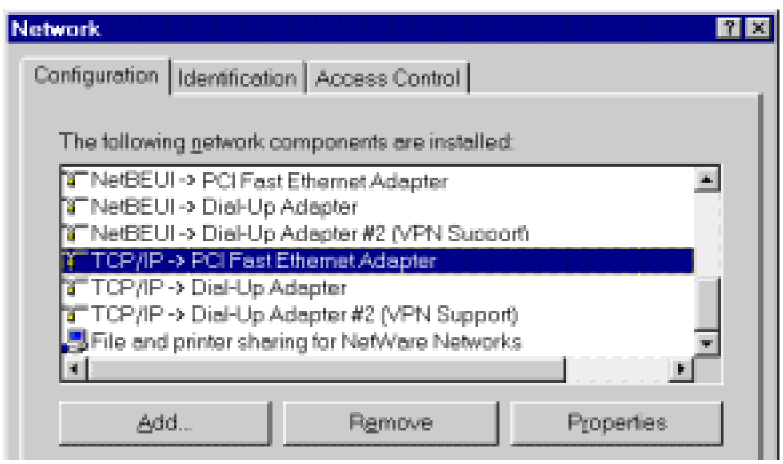


Figure B-1: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

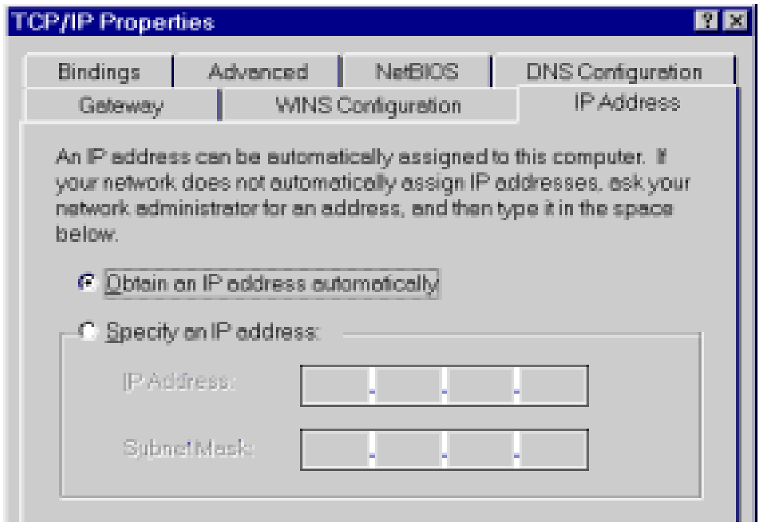


Figure B-2: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the VPN 800/2 Firewall Router.

Using "Specify an IP Address"

If your PC is already configured, check with your network administrator before making the following changes:

- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.
- On the *Gateway* tab, enter the VPN 800/2 Firewall Router's IP address in the *New Gateway* field and click *Add*, as shown below. (Your LAN administrator can advise you of the IP Address they assigned to the VPN 800/2 Firewall Router.)

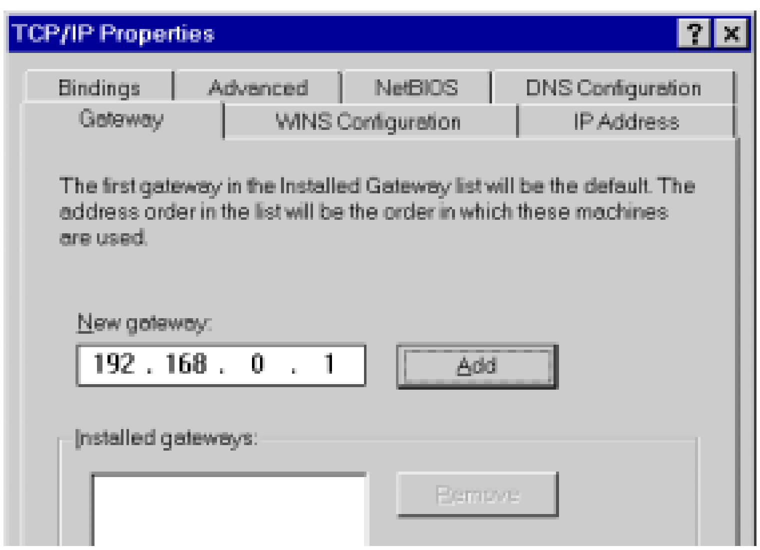


Figure B-3: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

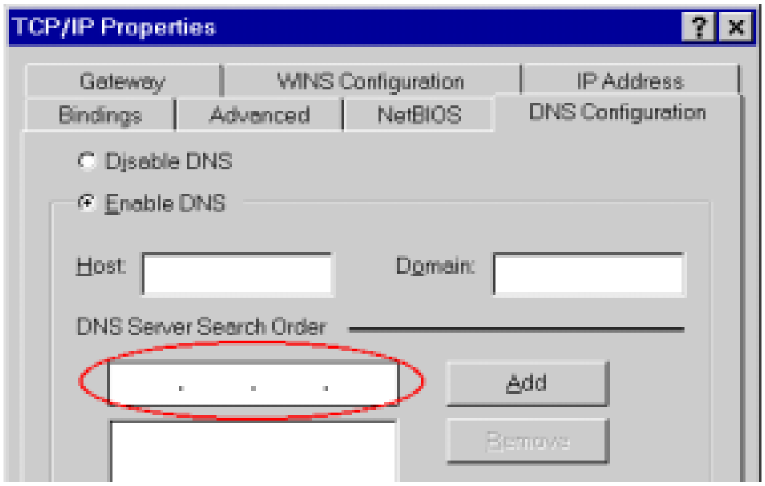


Figure B-4: DNS Tab (Win 95/98)

Checking TCP/IP Settings - Windows 2000:

1. Select *Control Panel - Network and Dial-up Connection*.
2. Right click the *Local Area Connection* icon and select *Properties*. You should see a screen like the following:

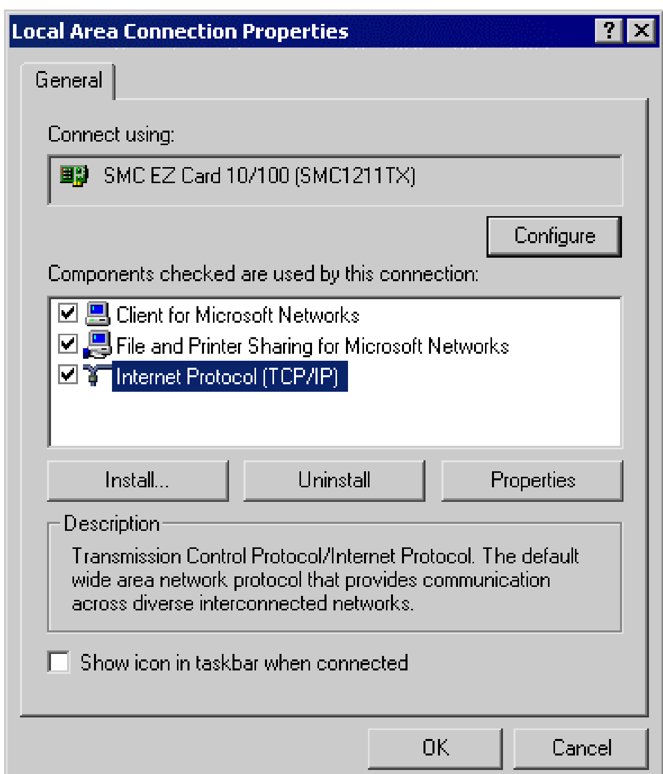


Figure B-5: Network Configuration (Win 2000)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

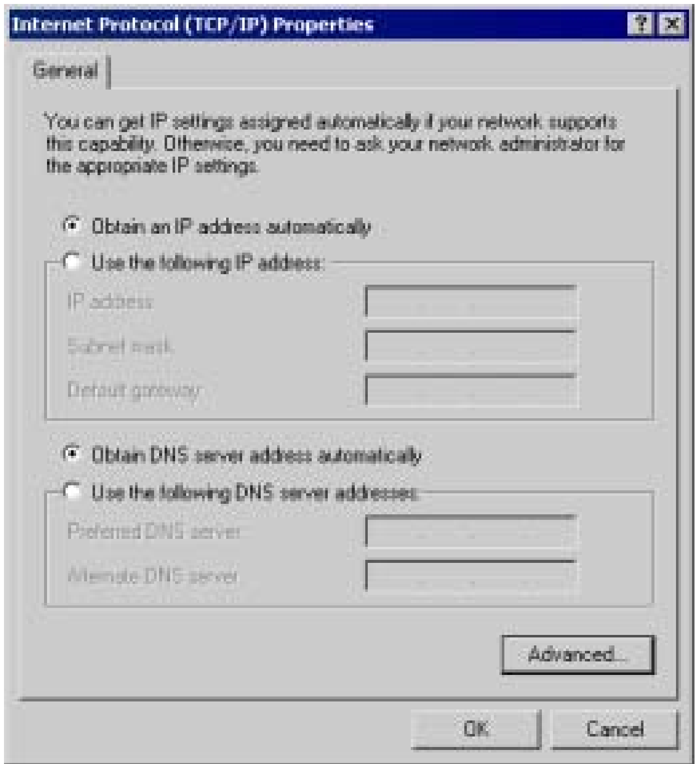


Figure B-6: TCP/IP Properties (Win 2000)

5. Ensure your TCP/IP settings are correct:

Using DHCP

To use DHCP, select the radio button *obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the VPN 800/2 Firewall Router.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes:

- Enter the VPN 800/2 Firewall Router's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the VPN 800/2 Firewall Router.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Checking TCP/IP Settings - Windows XP:

1. Select Control Panel - Network Connection.
2. Right click the *Local Area Connection* and choose *Properties*. You should see a screen like the following:

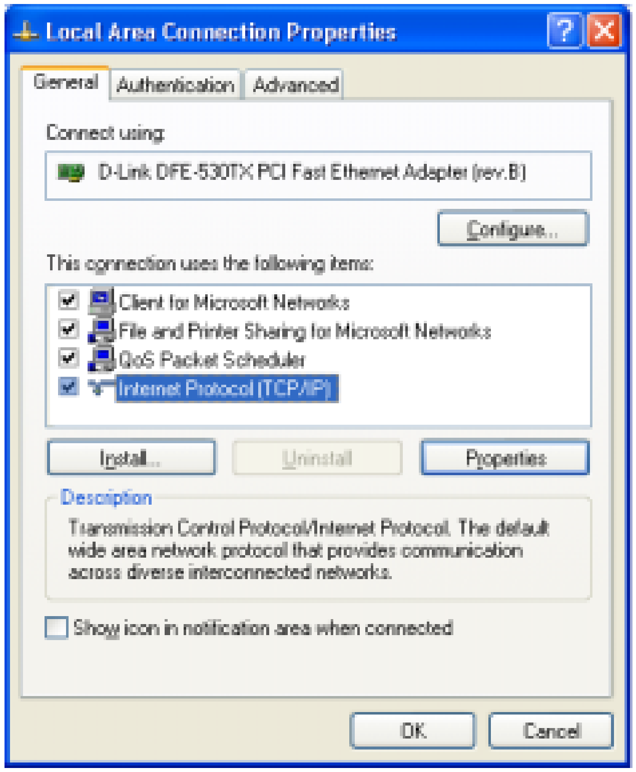


Figure B-7: Network Configuration (Windows XP)

3. Select the *TCP/IP* protocol for your network card.
4. Click on the *Properties* button. You should then see a screen like the following.

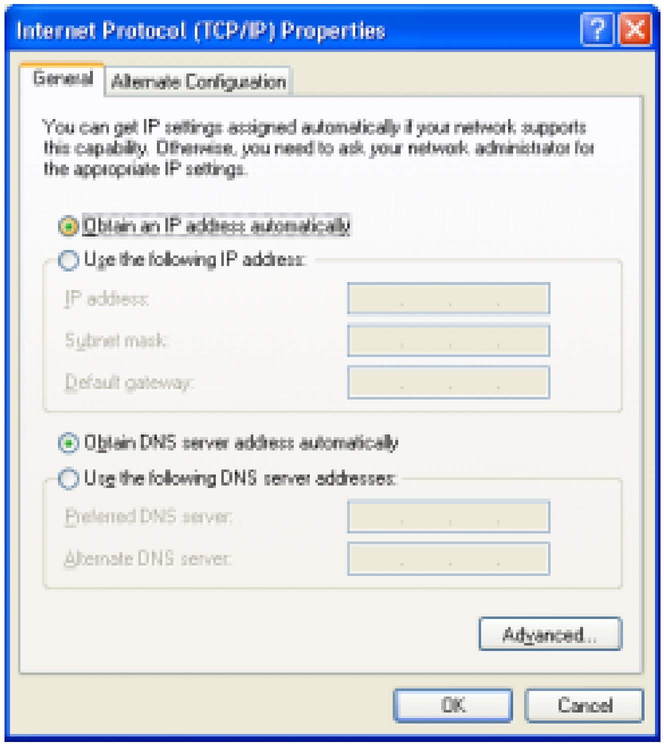


Figure B-8: TCP/IP Properties (Windows XP)

5. Ensure your TCP/IP settings are correct.

Using DHCP

To use DHCP, select the radio button *obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the VPN 800/2 Firewall Router.

Using a fixed IP Address ("Use the following IP Address")

If your PC is already configured, check with your network administrator before making the following changes.

- Enter the VPN 800/2 Firewall Router's IP address in the *Default gateway* field and click *OK*. (Your LAN administrator can advise you of the IP Address they assigned to the VPN 800/2 Firewall Router.)
- If the *DNS Server* fields are empty, select *Use the following DNS server addresses*, and enter the DNS address or addresses provided by your ISP, then click *OK*.

Appendix C
Troubleshooting

Overview

This chapter covers some common problems that may be encountered while using the VPN 800/2 Firewall Router and some possible solutions to them. If you follow the suggested steps and the VPN 800/2 Firewall Router still does not function properly, contact your dealer for further advice.

General Problems

Problem 1:	**Can't connect to the VPN 800/2 Firewall Router to configure it.**
Solution 1:	Check the following: • The Load Balancer is properly installed, LAN connections are OK, and it is powered ON. • Ensure that your PC and the VPN 800/2 Firewall Router are on the same network segment. (If you don't have a router, this must be the case.) • If your PC is set to "Obtain an IP Address automatically" (DHCP client), restart it. • If your PC uses a Fixed (Static) IP address, ensure that it is using an IP Address within the range 192.168.1.2 to 192.168.1.254 and thus compatible with the VPN 800/2 Firewall Router's default IP Address of 192.168.1.1. Also, the Network Mask should be set to 255.255.255.0 to match the VPN 800/2 Firewall Router. In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1:	**When I enter a URL or IP address I get a time out error.**
Solution 1:	A number of things could be causing this. Try the following troubleshooting steps. • Check if other PCs work. If they do, ensure that your PCs IP settings are correct. If using a Fixed (Static) IP Address, check the Network Mask, Default gateway and DNS as well as the IP Address. • If the PCs are configured correctly, but still not working, check the VPN 800/2 Firewall Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.) • If the VPN 800/2 Firewall Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.
Problem 2:	**Some applications do not run properly when using the VPN 800/2 Firewall Router.**

Solution 2:	The VPN 800/2 Firewall Router processes the data passing through it, so it is not transparent. Use the *Special Applications* feature to allow the use of Internet applications which do not function correctly. If this does solve the problem you can use the *DMZ* function. This should work with most applications, but: • It is a security risk, since the firewall is disabled for the *DMZ* PC. • Only one (1) PC can use this feature.